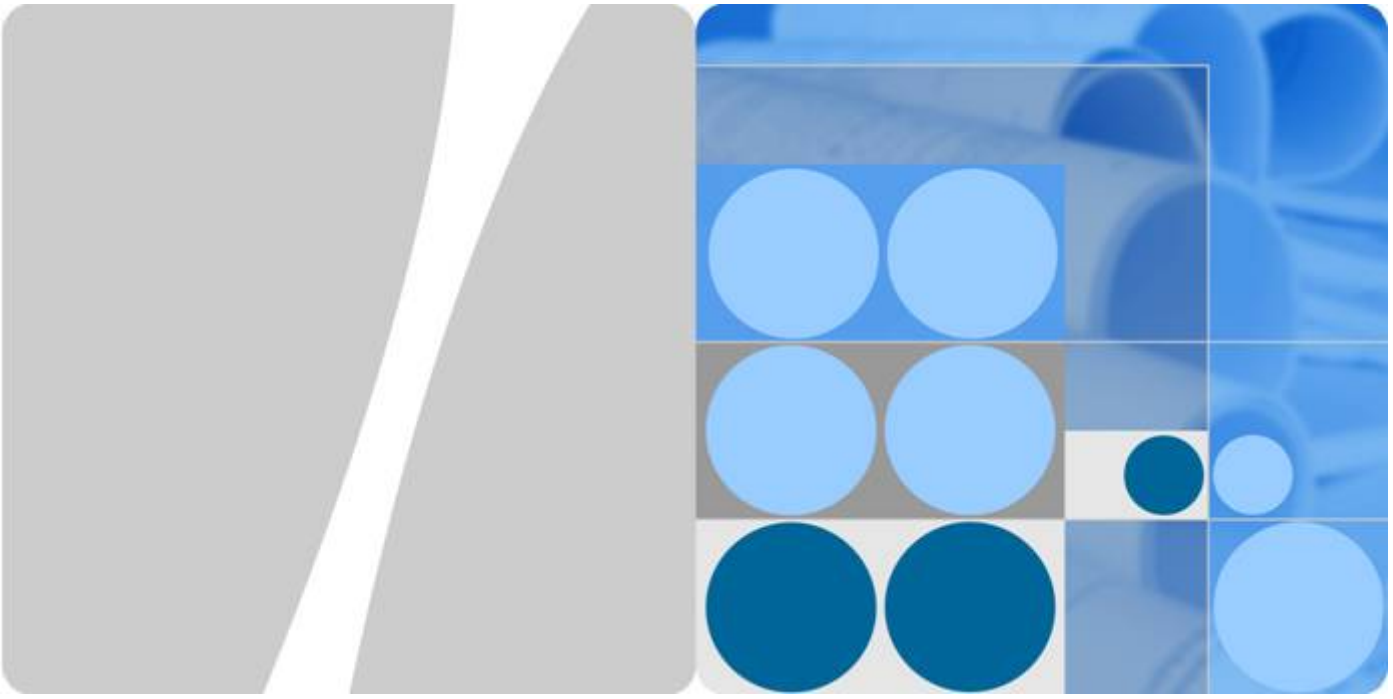


Huawei
AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600 系列企业路由器

V200R008

配置指南-QoS（通过命令行）

文档版本　04
发布日期　2017-06-22

华为技术有限公司

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://e.huawei.com

前 言

读者对象

本文档介绍了AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600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**	用于警示紧急的危险情形，若不避免，将会导致人员死亡或严重的人身伤害。
 **警告**	用于警示潜在的危险情形，若不避免，可能会导致人员死亡或严重的人身伤害。
 **小心**	用于警示潜在的危险情形，若不避免，可能会导致中度或轻微的人身伤害。
 **注意**	用于传递设备或环境安全警示信息，若不避免，可能会导致设备损坏、数据丢失、设备性能降低或其它不可预知的结果。 “注意”不涉及人身伤害。

符号	说明
说明	用于突出重要/关键信息、最佳实践和小窍门等。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

命令行格式约定

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。

产品软件和网管软件版本配套关系

产品软件和网管软件版本配套关系如下所示。

AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600产品软件版本	eSight网管软件版本	iManager U2000网管软件版本
V200R008（C20&C30）	V300R006C00	V200R016C50
V200R008C50	V300R007C00	V200R017C50

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 04 (2017-06-22)

该版本的更新如下：

修改：

- 8.2 配置基于ACL的报文过滤

文档版本 03 (2017-02-28)

该版本的更新如下：

修改：

- 4.5.2 配置MQC实现拥塞管理
- 4.6.2 配置MQC实现拥塞避免
- 6.4.3 应用流策略
- 2.5.1 配置端口信任的报文优先级
- 3.5.1 配置基于接口的流量监管

文档版本 02 (2016-11-25)

该版本的更新如下：

修改：

- 2.4 缺省配置
- 3.5.1 配置基于接口的流量监管
- 1.4.4 应用流策略

文档版本 01 (2016-07-30)

第一次正式发布。

目 录

1 MQC 配置

关于本章

通过配置MQC，按照某种规则对流量进行分类，并对同种类型的流量关联某种动作，实现针对不同业务的差分服务。

背景信息

说明

4GE-2S、4ES2G-S、4ES2GP-S和9ES2单板不支持MQC。

1.1 MQC简介
模块化QoS命令行MQC（Modular QoS Command-Line Interface）是指通过将具有某类共同特征的报文划分为一类，并为同一类报文提供相同的服务，也可以对不同类的报文提供不同的服务。

1.2 规格
介绍MQC的规格。

1.3 配置注意事项
介绍部署MQC的注意事项。

1.4 配置MQC
介绍MQC详细的配置过程。

1.5 维护MQC
使能了流量统计功能后，可以查看MQC配置的统计信息，分析报文的通过和丢弃情况。

1.6 参考信息

1.1 MQC 简介

模块化QoS命令行MQC（Modular QoS Command-Line Interface）是指通过将具有某类共同特征的报文划分为一类，并为同一类报文提供相同的服务，也可以对不同类的报文提供不同的服务。

随着网络中QoS业务的不断丰富，在网络规划时若要实现对不同流量（如不同业务或不同用户）的差分服务，会使部署比较复杂。MQC的出现，使用户能对网络中的流量进行精细化处理，用户可以更加便捷的针对自己的需求对网络中的流量提供不同的服务，完善了网络的服务能力。

MQC 三要素

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

- 流分类

  流分类用来定义一组流量匹配规则，以对报文进行分类。流分类规则如表1-1所示：

表 1-1 流分类的分类规则

层级	分类规则
二层	● 目的MAC地址 ● 源MAC地址 ● VLAN报文外层Tag的ID信息 ● VLAN报文外层Tag的802.1p优先级 ● VLAN报文内层Tag的ID信息 ● VLAN报文内层Tag的802.1p优先级 ● 基于二层封装的协议字段 ● MPLS报文的EXP优先级（AR1200&AR2200&AR3200&AR3600） ● FR报文中的DE标志位 ● FR报文中的DLCI信息 ● ATM报文中的PVC信息 ● ACL 4000～4999匹配的字段

层级	分类规则
三层	● IP报文的DSCP优先级 ● IP报文的IP优先级 ● IP协议类型（IPv4协议或IPv6协议） ● RTP端口号 ● TCP报文的TCP-Flag标志 ● IPv4报文长度 ● IPSec策略的QoS group ● ACL 2000～3999匹配的字段 ● ACL6 2000～3999匹配的字段
其他	● 所有报文 ● 入接口 ● 出接口 ● SAC ● 用户组

流分类中各规则之间的关系分为：and或or，缺省情况下的关系为or。

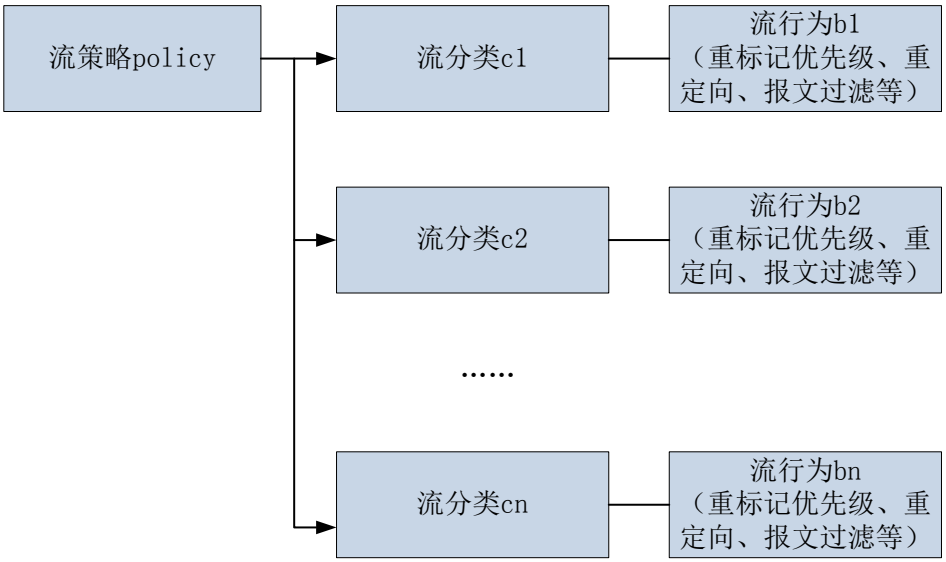
- and：当流分类中包含ACL规则时，报文必须匹配其中一条ACL规则以及所有非ACL规则才属于该类；当流分类中没有ACL规则时，报文必须匹配所有非ACL规则才属于该类。
- or：报文只要匹配了流分类中的一个规则，设备就认为报文属于此类。

- 流行为

  流行为用来定义针对某类报文所做的动作。
- 流策略

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

图 1-1 流策略绑定多个流分类和流行为

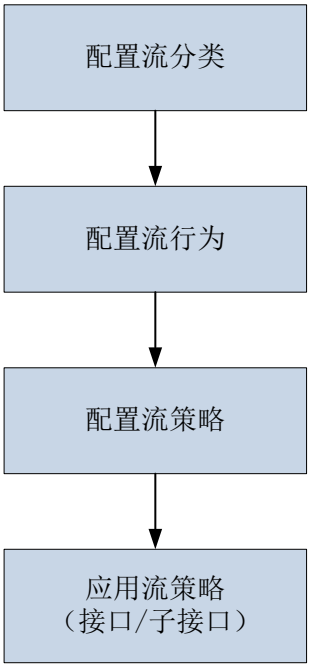


MQC 配置流程

MQC配置流程如图1-2所示。

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

图 1-2 MQC 配置流程



相关资料

视频：**AR G3系列路由器QOS特性介绍**

1.2 规格

介绍MQC的规格。

MQC的规格如表1-2所示。

表 1-2 MQC 规格

项目	规格
设备支持流分类个数	1024
一个流分类支持的if-match规则数	1024
设备支持的流行为数	1024
设备支持的流策略数	1024
一个流策略绑定的流分类数	1024

1.3 配置注意事项

介绍部署MQC的注意事项。

- 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，请根据设备款型联系华为办事处申请并购买如下License：
  - 对于AR150&AR160&AR200系列设备：AR150&160&200安全业务增值包
  - 对于AR1200系列设备：AR1200安全业务增值包
  - 对于AR2200系列设备：AR2200安全业务增值包
  - 对于AR3200系列设备：AR3200安全业务增值包
  - 对于AR3600系列设备：AR3600安全业务增值包
- 定义基于应用协议的匹配规则前，必须使能SAC功能并加载特征库。
- 当使用ACL作为流分类规则匹配源IP地址时，通过在接口下的**qos pre-nat**配置NAT预分类功能，可以将NAT转换前的私网IP地址信息携带到出接口，即可实现基于私网IP地址的分类，从而对来自不同私网IP地址的报文提供差分服务。
- 流行为中，**permit**动作和其他流动作一起配置时，将依次执行这些动作；**deny**动作和其他流动作互斥，即使配置其它动作也不会生效（流量统计和流镜像除外）。
- 为匹配ACL规则的报文指定报文过滤动作时，如果此ACL中的rule规则配置为**permit**，则设备对此报文采取的动作由流行为中配置的**deny**或**permit**决定；如果此ACL中的rule规则配置为**deny**，则无论流行为中配置了**deny**或**permit**，此报文都被丢弃。
- 如果在流行为中配置了**remark 8021p**、**remark mpls-exp**、**remark dscp**，未配置**remark local-precedence**，则报文中的本地优先级会被标记为0。
- 与重定向联动的NQA测试例必须为ICMP类型，具体配置请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列企业路由器 NQA配置》中的“配置ICMP测试”部分。

- 重定向配置对IPv6报文中的Hop-by-Hop报文不生效。
- 目前设备仅支持重定向到3G Cellular接口和Dialer接口（对于MPOEOA链路方式，不支持重定向到Dialer接口）。
- 包含以下流行为的流策略只能应用在设备WAN接口的出方向：
  - 流量整形
  - 自适应流量整形
  - 拥塞管理
  - 拥塞避免
- 设备配置分片后，若流分类中的规则包含**non-first-fragment**，对于发送到本机的分片报文流策略无法进行**car**或统计动作。

1.4 配置 MQC

介绍MQC详细的配置过程。

1.4.1 配置流分类

背景信息

配置流分类，可以将匹配一定规则的报文归为一类，对匹配同一流分类的报文进行相同的处理，是实现差分服务的前提和基础。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]，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”，指定该逻辑关系后：
   - 当流分类中有ACL规则时，报文必须匹配其中一条ACL规则以及所有非ACL规则才属于该类。
   - 当流分类中没有ACL规则时，则报文必须匹配所有非ACL规则才属于该类。

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

   缺省情况下，流分类中各规则之间的关系为“逻辑或”。
3. 请根据实际情况配置流分类中的匹配规则。

匹配规则	命令
外层VLAN ID	**if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*]
QinQ报文内层VLAN ID	**if-match cvlan-id** *start-vlan-id* [**to** *end-vlan-id*]
VLAN报文802.1p优先级	**if-match 8021p** *8021p-value* &<1-8>
QinQ报文内层VLAN的802.1p优先级	**if-match cvlan-8021p** *8021p-value* &<1-8>

匹配规则	命令
MPLS报文EXP优先级（AR1200&AR2200&AR3200&AR3600系列）	**if-match mpls-exp** *exp-value* &<1-8>
目的MAC地址	**if-match destination-mac** *mac-address* [**mac-address-mask** *mac-address-mask*]
源MAC地址	**if-match source-mac** *mac-address* [**mac-address-mask** *mac-address-mask*]
FR报文中的DLCI信息	**if-match dlci** *start-dlci-number* [**to** *end-dlci-number*]
FR报文中的DE标志位	**if-match fr-de**
以太网帧头中协议类型字段	**if-match l2-protocol** { **arp** | **ip** | **mpls** | **rarp** | *protocol-value* }
所有报文	**if-match any**
IP报文的DSCP优先级	**if-match** [**ipv6**] **dscp** *dscp-value* &<1-8> **说明** 如果流策略中配置了匹配DSCP，则SAE220（WSIC）和SAE550（XSIC）单板不支持**redirect ip-nexthop** *ip-address* **post-nat**动作。
IP报文的IP优先级	**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 [ipv6] dscp**和**if-match ip-precedence**。
报文三层协议类型	**if-match protocol** { **ip** | **ipv6** }
指定QoS group索引的IPSec报文	**if-match qos-group** *qos-group-value*
IPv4报文长度	**if-match packet-length** *min-length* [**to** *max-length*]
ATM报文中的PVC信息	**if-match pvc** *vpi-number/vci-number*
RTP端口号	**if-match rtp start-port** *start-port-number* **end-port** *end-port-number*
TCP报文SYN Flag	**if-match tcp syn-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** }*
入接口	**if-match inbound-interface** *interface-type interface-number*
出接口	**if-match outbound-interface Cellular** *interface-number:channel*

匹配规则	命令
ACL规则	**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。 ● 当使用ACL作为流分类规则匹配源IP地址时，通过在接口下的**qos pre-nat**配置NAT预分类功能，可以将NAT转换前的私网IP地址信息携带到出接口，即可实现基于私网IP地址的分类，从而对来自不同私网IP地址的报文提供差分服务。
ACL6规则	**if-match ipv6 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。 ● 当使用ACL作为流分类规则匹配源IP地址时，通过在接口下的**qos pre-nat**配置NAT预分类功能，可以将NAT转换前的私网IP地址信息携带到出接口，即可实现基于私网IP地址的分类，从而对来自不同私网IP地址的报文提供差分服务。
应用协议	**if-match application** *application-name* [**user-set** *user-set-name*] [**time-range** *time-name*] **说明** 定义基于应用协议的匹配规则前，必须使能SA功能并加载特征库。
SA协议组	**if-match category** *category-name* [**user-set** *user-set-name*] [**time-range** *time-name*] **说明** ● 定义基于应用协议的匹配规则前，必须使能SA功能并加载特征库。
用户组	**if-match user-set** *user-set-name* [**time-range** *time-range-name*]

4. 执行命令**quit**，退出流分类视图。

1.4.2 配置流行为

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，保证接口正常工作。

背景信息

设备支持报文过滤、重标记优先级、重定向、流量监管、流量统计等动作。

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，或进入已存在的流行为视图。

步骤3 请根据实际情况定义流行为中的动作，只要各动作不冲突，都可以在同一流行为中配置。

动作	命令
配置报文过滤	**deny** | **permit**
配置报文所属的QoS组	**remark qos-group** *qos-group-value*
配置MQC实现重标记优先级	**remark 8021p** *8021p-value* **remark cvlan-8021p** *8021p-value* **remark dscp** { *dscp-name* | *dscp-value* } **remark mpls-exp** *exp-value*（AR1200&AR2200&AR3200&AR3600系列） **remark fr-de** *fr-de-value* **remark local-precedence** *local-precedence-value* **说明** 如果在流行为中配置了**remark 8021p**、**remark mpls-exp**、**remark dscp**，未配置**remark local-precedence**，报文中的本地优先级会被标记为0。
配置MQC实现流量监管	**car cir** { *cir-value* | **pct** *cir-percentage* } [**pir** { *pir-value* | **pct** *pir-percentage* }] [**cbs** *cbs-value* **pbs** *pbs-value*] [**share**] [**mode** { **color-blind** | **color-aware** }] [**green** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] [**yellow** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] [**red** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] **说明** AR100&AR120&AR150&AR160&AR200系列不支持**remark-mpls-exp** *exp-value*参数。
配置MQC实现流量整形	**gts cir** { *cir-value* [**cbs** *cbs-value*] | **pct** *pct-value* } [**queue-length** *queue-length*]
配置MQC实现自适应流量整形	**gts adaptation-profile** *adaptation-profile-name*

动作	命令
配置MQC实现拥塞管理	**queue af bandwidth** { *bandwidth* | [**remaining**] **pct** *percentage* } **queue ef bandwidth** { *bandwidth* [**cbs** *cbs-value*] | **pct** *percentage* [**cbs** *cbs-value*] } **queue llq bandwidth** { *bandwidth* [**cbs** *cbs-value*] | **pct** *percentage* [**cbs** *cbs-value*] } **queue wfq** [**queue-number** *total-queue-number*] **queue-length** { **bytes** *bytes-value* | **packets** *packets-value* }*
配置MQC实现拥塞避免	**drop-profile** *drop-profile-name*
配置MQC实现Netstream统计采样	**ip netstream sampler** { **fix-packets** *packet-interval* | **fix-time** *time-interval* | **random-packets** *packet-interval* | **random-time** *time-interval* } { **multicast** | **rpf-failure** | **unicast** }* **说明** ● IPv6和MPLS报文不支持配置Netstream统计采样功能，因此对应的流分类规则不能包含IPv6或MPLS关键字。 ● V200R008C50及以后版本，二层VE接口不支持该功能。
配置单播策略路由	**redirect ip-nexthop** *ip-address* [**track** { **nqa** *admin-name test-name* | **ip-route** *ip-address* { *mask* | *mask-length* } }] [**post-nat**] [**discard**] **说明** 如果流策略中配置了匹配DSCP，则SAE220（WSIC）和SAE550（XSIC）单板不支持**redirect ip-nexthop** *ip-address* **post-nat**动作。 **redirect ipv6-nexthop** *ipv6-address* [**track** { **nqa** *nqa-admin nqa-name* | **ipv6-route** *ipv6﹣address mask-length* }] [**discard**] **redirect interface** *interface-type interface-number* [**track** { **nqa** *admin-name test-name* | **ip-route** *ip-address* { *mask* | *mask-length* } | **ipv6-route** *ipv6-address mask-length* }] [**discard**] **redirect vpn-instance** *vpn-instance-name* **说明** V200R008C50及以后版本，二层VE接口不支持该功能。
配置绑定子策略	**traffic-policy** *policy-name*
配置流量统计	**statistic enable**
配置MQC实现URL过滤	**url-filter-profile** *profile-name*

说明

当接口加入网桥时，在接口的入方向定义流行为，流行为的动作中仅支持:

- 创建重标记VLAN报文802.1p优先级。
- 配置MQC实现流量监管。
- 配置流量统计。

步骤4 执行命令**quit**，退出流行为视图。

----结束

1.4.3 配置流策略

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

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**traffic policy** *policy-name*，创建一个流策略并进入流策略视图，或进入已存在的流策略视图。
3. 执行命令**classifier** *classifier-name* **behavior** *behavior-name*，在流策略中为指定的流分类配置所需流行为，即绑定流分类和流行为。
4. 执行命令**quit**，退出流策略视图。
5. 执行命令**quit**，退出系统视图。

1.4.4 应用流策略

前置任务

在应用流策略之前，需要完成以下任务：

- 配置流策略

操作步骤

- 在接口下应用流策略
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number* [*.subinterface-number*]，进入接口视图。
  c. 执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，在接口的入方向或出方向应用流策略。
- 在安全域间应用流策略

  说明

  仅AR100&AR120&AR150&AR160&AR200系列支持此步骤。

  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**firewall interzone** *zone-name1 zone-name2*，创建安全域间并进入安全域间视图。

     缺省情况下，未创建安全域间。

     创建安全域间必须指定两个已存在的安全区域。
  c. 执行命令**traffic-policy** *policy-name*，在安全域间绑定流策略。

     缺省情况下，安全域间没有绑定流策略。

- 在BD下应用流策略

  说明

  仅在V200R008C30及之后版本，AR100&AR120&AR150&AR160&AR200&AR1200系列和AR2220E支持此步骤。

  a. 执行命令**system-view**，进入系统视图。

  b. 执行命令**bridge-domain** *bd-id*，创建广播域BD（Bridge Domain）并进入BD视图。

  缺省情况下，没有创建广播域BD。

  c. 执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，在BD下应用流策略。

  缺省情况下，BD下没有应用任何流策略。

1.4.5 检查配置结果

操作步骤

- 执行命令**display traffic classifier user-defined** [*classifier-name*]，查看已配置的流分类信息。
- 执行命令**display traffic behavior** { **system-defined** | **user-defined** } [*behavior-name*]，查看已配置的流行为信息。
- 执行命令**display traffic policy user-defined** [*policy-name* [**classifier** *classifier-name*]]，查看流策略的配置信息。
- 执行命令**display traffic-policy applied-record** [*policy-name*]，查看指定流策略的应用记录。

1.5 维护 MQC

使能了流量统计功能后，可以查看MQC配置的统计信息，分析报文的通过和丢弃情况。

1.5.1 查看 MQC 统计信息

背景信息

MQC统计信息即流策略统计信息。当用户需要了解接口或BD下应用指定流策略后报文通过和被丢弃的情况时，可以查看流策略统计信息。

查看流策略统计信息时，MQC配置必须存在且已经包含**statistic enable**动作。

操作步骤

- 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* [**son-class** *son-class-name*]]]或**display traffic policy statistics interface virtual-template** *vt-number* **virtual-access** *va-number* { **inbound** | **outbound** } [**verbose** { **classifier-base** | **rule-base** } [**class** *classifier-name* [**son-class** *son-class-name*]]]，查看指定接口下应用流策略后的报文统计信息。

- 执行命令**display traffic policy statistics bridge-domain** *bd-id* { **inbound** | **outbound** } [**verbose** { **classifier-base** | **rule-base** } [**class** *classifier-name*]]，查看指定BD下应用流策略后的报文统计信息。

  说明

  仅在V200R008C30及之后版本，AR100&AR120&AR150&AR160&AR200&AR1200系列和AR2220E支持此步骤。

----结束

1.5.2 清除 MQC 统计信息

背景信息

MQC统计信息即流策略统计信息。当用户需要对接口或BD下流策略的统计信息重新进行统计时，可以执行以下命令，清除之前的流策略统计信息。

注意

清除流策略统计信息后，以前的统计信息将无法恢复，请在清除之前仔细确认。

操作步骤

- 用户视图下执行命令**reset traffic policy statistics interface** *interface-type interface-number* [**pvc** *vpi-number/vci-number* | **dlci** *dlic-number*] { **inbound** | **outbound** }或**reset traffic policy statistics interface virtual-template** *vt-number* **virtual-access** *va-number* { **inbound** | **outbound** }，清除指定接口下应用流策略后的报文统计信息。
- 用户视图下执行命令**reset traffic policy statistics bridge-domain** *bd-id* { **inbound** | **outbound** }，清除指定BD下应用流策略后的报文统计信息。

  说明

  仅在V200R008C30及之后版本，AR100&AR120&AR150&AR160&AR200&AR1200系列和AR2220E支持此步骤。

----结束

1.6 参考信息

介绍QoS特性的相关参考资料。

文档	描述	备注
RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	-
RFC 2475	An Architecture for Differentiated Services	-
RFC 2597	Assured Forwarding PHB Group	-

文档	描述	备注
RFC 2598	An Expedited Forwarding PHB	-
RFC 2697	A Single Rate Three Color Marker	-
RFC 2698	A Two Rate Three Color Marker	-

2 优先级映射配置

关于本章

优先级映射配置介绍优先级映射等基本概念并介绍优先级映射的配置方法、配置示例以及常见配置错误。

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

2.2 原理描述

2.3 应用场景

2.4 缺省配置
介绍优先级映射表和缺省取值。

2.5 配置优先级映射
配置优先级映射后，设备将根据报文携带的优先级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。

2.6 配置举例
通过示例介绍如何应用优先级映射。配置示例中包括组网需求、配置注意事项、配置思路等。

2.7 常见配置错误
介绍优先级映射配置的常见错误。

2.8 FAQ
介绍配置优先级映射的FAQ。

2.9 参考信息

2.1 优先级映射概述

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

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

2.2 原理描述

优先级映射

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

优先级映射实现从QoS优先级到内部优先级（或者本地优先级）或从内部优先级到QoS优先级的映射，并利用DiffServ域来管理和记录QoS优先级和服务等级之间的映射关系。对于进入设备的报文，设备将报文携带的优先级或者端口优先级映射为内部优先级，然后根据内部优先级与队列之间的映射关系确定报文进入的队列，从而针对队列进行流量整形、拥塞避免、队列调度等处理，并可以根据配置修改报文发送出去时所携带的优先级，以便其他设备根据报文的优先级提供相应的QoS服务。

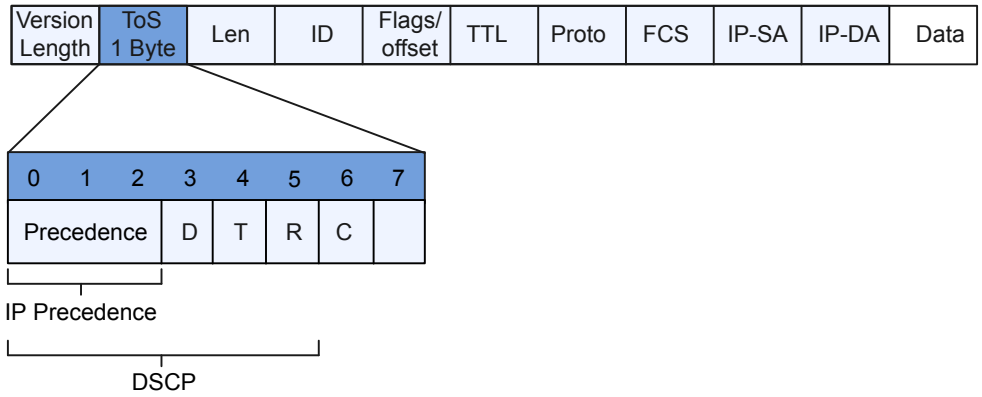
QoS 优先级字段

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

- Precedence字段

  根据RFC791定义，IP报文头ToS（Type of Service）域由8个比特组成，其中3个比特的Precedence字段标识了IP报文的优先级，Precedence在报文中的位置如**图2-1**所示。

图 2-1 IP Precedence/DSCP 字段



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

除了Predecence字段外，ToS域中还包括D、T、R三个比特：

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

- DSCP字段

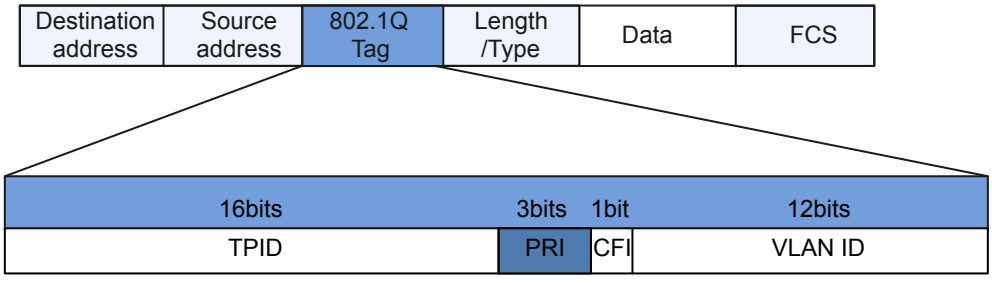
  RFC1349重新定义了IP报文中的ToS域，增加了C比特，表示传输开销（Monetary Cost）。之后，IETF DiffServ工作组在RFC2474中将IPv4报文头ToS域中的比特0～5重新定义为DSCP，并将ToS域改名为DS（Differentiated Service）字节。DSCP在报文中的位置如图2-1所示。

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

- VLAN帧头中的802.1p优先级

  通常二层设备之间交互VLAN帧。根据IEEE 802.1Q定义，VLAN帧头中的PRI字段（即802.1p优先级），或称CoS（Class of Service）字段，标识了服务质量需求。VLAN帧中的PRI字段位置如图2-2所示。

图 2-2 VLAN 帧中的 802.1p 优先级

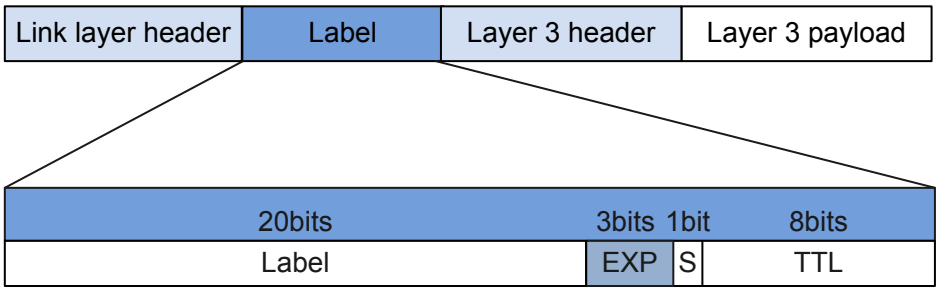


在802.1Q头部中包含3比特长的PRI字段。PRI字段定义了8种业务优先级CoS，按照优先级从高到低顺序取值为7、6、5、4、3、2、1和0。

- MPLS EXP字段

  MPLS报文与普通的IP报文相比增加了标签信息。标签的长度为4个字节，封装结构如图2-3所示。

  图 2-3 MPLS 标签的封装格式

  标签共有4个域：

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

  对于MPLS报文，通常将标签信息中的EXP域作为MPLS报文的CoS域，与IP网络的ToS域等效，用来区分数据流量的服务等级，以支持MPLS网络的DiffServ。EXP字段表示8个传输优先级，按照优先级从高到低顺序取值为7、6、5、4、3、2、1和0。

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

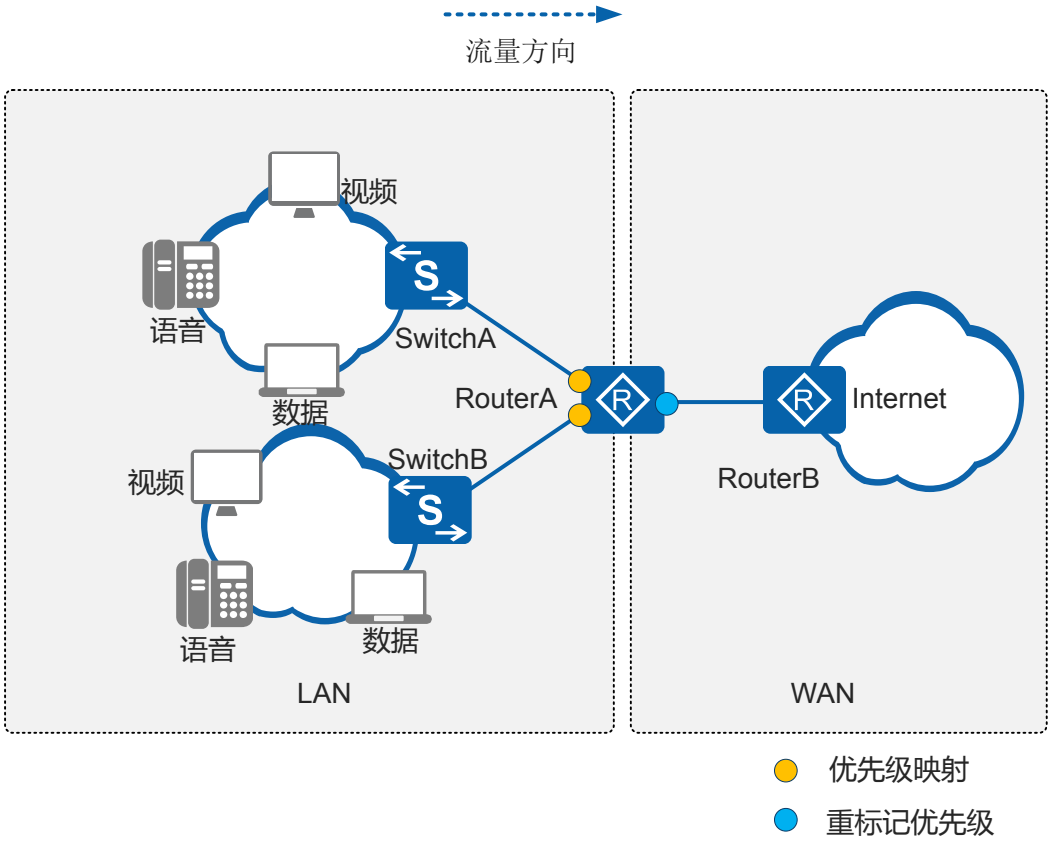
2.3 应用场景

组网需求

不同网络中的报文使用不同的优先级字段，例如LAN侧网络的报文使用802.1p优先级，WAN侧网络中的报文使用DSCP优先级。如图2-4所示，企业网用户的语音、视频、数据业务通过RouterA接入WAN侧网络。报文在LAN侧网络传输时使用802.1p优先级进行标识，在RouterA入方向上将报文的802.1p优先级映射到某优先级字段，以便RouterA根据映射结果对报文进行差分服务。当报文进入WAN侧网络时，需要使用

DSCP优先级进行标识，此时可以在RouterA上根据报文的802.1p优先级来重标记报文的DSCP优先级值。

图 2-4 优先级映射应用组网图



业务部署

- RouterA根据802.1p优先级将报文送入不同的队列进行差分服务。
- RouterA配置优先级映射表，将802.1p优先级映射为DSCP优先级，以便报文在出RouterA进入WAN侧网络时可以根据802.1p优先级重标记DSCP优先级，可以让后续设备根据DSCP优先级进行差分服务。

2.4 缺省配置

介绍优先级映射表和缺省取值。

设备提供多张优先级映射表，分别对应相应的优先级映射关系。缺省情况如下：

- AR100&AR120&AR150&AR160&AR200系列、AR1200系列、AR2204、AR2220E和AR2220L支持的802.1p到DSCP的映射关系如表2-1，802.1p到802.1p的优先级映射保持不变；DSCP到802.1p的映射关系如表2-3，DSCP到DSCP的优先级映射保持不变；MPLS EXP到MPLS EXP的优先级映射保持不变。

- AR2201-48FE、AR2204-24GE、AR2204-27GE、AR2204-27GE-P、AR2204-48GE-P、AR2204-51GE-P、AR2204-51GE、AR2204-51GE-R、AR2204E、AR2204E-D、AR2202-48FE、AR2220、AR2240C、AR2240和AR3200&AR3600系列支持的802.1p到DSCP、到本地优先级的映射关系如**表2-2**，802.1p到802.1p的优先级映射保持不变；DSCP到802.1p、到本地优先级的映射关系如**表2-4**，DSCP到DSCP的优先级映射保持不变；MPLS EXP到本地优先级的映射关系如**表2-5**，MPLS EXP到MPLS EXP的优先级映射保持不变。

表 2-1 802.1p 到 DSCP 的映射关系表（AR100&AR120&AR150&AR160&AR200 系列、AR1200 系列、AR2204、AR2220E 和 AR2220L）

Input 802.1p	Output DSCP
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

表 2-2 802.1p 到本地优先级、DSCP 的映射关系表（AR2201-48FE、AR2204-24GE、AR2204-27GE、AR2204-27GE-P、AR2204-48GE-P、AR2204-51GE-P、AR2204-51GE、AR2204-51GE-R、AR2204E、AR2204E-D、AR2202-48FE、AR2220、AR2240C、AR2240 和 AR3200&AR3600 系列）

Input 802.1p	Output DSCP	Output LP
0	0	0
1	8	1
2	16	2
3	24	3
4	32	4
5	40	5
6	48	6
7	56	7

表 2-3 DSCP 到 802.1p 的映射关系表（AR100&AR120&AR150&AR160&AR200 系列、AR1200 系列、AR2204、AR2220E 和 AR2220L）

Input DSCP	Output 802.1p
0～7	0
8～15	1
16～23	2
24～31	3
32～39	4
40～47	5
48～55	6
56～63	7

表 2-4 DSCP 到本地优先级和 802.1p 的映射关系表（AR2201-48FE、AR2204-24GE、AR2204-27GE、AR2204-27GE-P、AR2204-48GE-P、AR2204-51GE-P、AR2204-51GE、AR2204-51GE-R、AR2204E、AR2204E-D、AR2202-48FE、AR2220、AR2240C、AR2240 和 AR3200&AR3600 系列）

Input DSCP	Output 802.1p	Output LP
0～7	0	0
8～15	1	1
16～23	2	2
24～31	3	3
32～39	4	4
40～47	5	5
48～55	6	6
56～63	7	7

表 2-5 MPLS EXP 到本地优先级的映射关系表（AR2201-48FE、AR2204-24GE、AR2204-27GE、AR2204-27GE-P、AR2204-48GE-P、AR2204-51GE-P、AR2204-51GE、AR2204-51GE-R、AR2204E、AR2204E-D、AR2202-48FE、AR2220、AR2240C、AR2240 和 AR3200&AR3600 系列）

Input MPLS EXP	Output LP
0	0
1	1

Input MPLS EXP	Output LP
2	2
3	3
4	4
5	5
6	6
7	7

2.5 配置优先级映射

配置优先级映射后，设备将根据报文携带的优先级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。

前置任务

配置优先级映射之前，需要完成以下任务：

- 配置相关接口的链路层属性，保证接口正常工作

2.5.1 配置端口信任的报文优先级

背景信息

设备提供三种报文优先级信任模式，可以根据需要选择其中一种进行配置：

- 信任报文的802.1p优先级
  - 对于带VLAN Tag的报文，设备根据报文携带的802.1p优先级查找优先级映射表，确定报文进入的队列，并可以修改报文的优先级值。
  - 对于不带VLAN Tag的报文，设备将使用端口优先级作为802.1p优先级，查找优先级映射表，确定报文进入的队列，并可以修改报文的优先级值。
- 信任报文的DSCP优先级

  设备按照报文携带的DSCP优先级查找DSCP优先级映射表，确定报文进入的队列，并可以修改报文的优先级值。
- 信任报文的MPLS EXP优先级

  设备按照报文携带的MPLS EXP优先级查找MPLS EXP优先级映射表，确定报文进入的队列，并可以修改报文的优先级值。

  说明

  - AR100&AR120&AR150&AR160&AR200系列不支持信任报文的MPLS EXP优先级。
  - V200R008C30及以前版本，仅WAN侧接口支持配置信任报文的MPLS EXP优先级。V200R008C50及以后版本，设备支持在WAN侧接口和二层VE接口配置信任报文的MPLS EXP优先级。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

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

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

缺省情况下，端口不信任任何报文优先级，使用端口优先级。

说明

- 对于AR100&AR120&AR150&AR160（除AR161、AR161W、AR169、AR161G-L、AR161G-Lc、AR161EW、AR161EW-M1、AR161G-U、AR169G-L、AR169EW、AR169CVW、AR169CVW-4B4S、AR169EGW-L、AR169W-P-M9、AR169RW-P-M9和AR169-P-M9）&AR200系列、AR1200系列、AR2204或AR2220L&AR2220E来说，未配置**override**属性时，报文按照指定优先级映射后，报文的802.1p值被修改成映射后的值，报文的DSCP值保持不变；配置**override**属性时，报文按照指定优先级映射后，报文的802.1p值、DSCP值均被修改成映射后的值。
- 对于AR2201-48FE、AR2204-24GE、AR2204-27GE、AR2204-27GE-P、AR2204-48GE-P、AR2204-51GE-P、AR2204-51GE、AR2204-51GE-R、AR2204E、AR2204E-D、AR2202-48FE、AR2220、AR2240C、AR2240或AR3200&AR3600系列来说，未配置**override**属性时，报文按照指定优先级映射后，报文的优先级并不修改；配置**override**属性时，报文按照指定优先级映射后，报文的802.1p值、DSCP值均被修改成映射后的值。

----结束

2.5.2 （可选）配置端口优先级

背景信息

在以下两种情况下，会使用到端口优先级：

- 端口收到了不带VLAN Tag的报文，则在设备内部转发时根据端口优先级进行转发。
- 端口配置的是信任报文的802.1p优先级，收到不带VLAN Tag的报文时，设备将端口优先级作为802.1p优先级，查找802.1p优先级到各优先级映射表，确定报文进入的队列。

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

2.5.3 配置优先级映射表

背景信息

设备根据报文自带的优先级或端口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。设备支持802.1p、DSCP和MPLS EXP优先级映射之间的映射，以及将802.1p、DSCP或MPLS EXP优先级映射为本地优先级。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 在不同设备上选择相应命令，进入优先级映射表视图。

- 在AR100&AR120&AR150&AR160&AR200系列上，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。
- 在AR1200系列、AR2240C、AR2204、AR2220E或AR2220L上，执行命令**qos map-table** { **dot1p-dot1p** | **dot1p-dscp** | **dscp-dot1p** | **dscp-dscp** | **exp-exp** }，进入优先级映射表视图。
- 在AR2201-48FE、AR2204-24GE、AR2204-27GE、AR2204-27GE-P、AR2204-48GE-P、AR2204-51GE-P、AR2204-51GE、AR2204-51GE-R、AR2204E、AR2204E-D、AR2202-48FE、AR2220、AR2240或AR3200&AR3600系列上，执行命令**qos map-table** { **dot1p-dot1p** | **dot1p-dscp** | **dot1p-lp** | **dscp-dot1p** | **dscp-dscp** | **dscp-lp** | **exp-exp** | **exp-lp** }，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

2.5.4 检查配置结果

操作步骤

- 在不同设备上选择相应命令，查看当前的各优先级间的映射关系。
  - 在AR100&AR120&AR150&AR160&AR200系列上，执行命令**display qos map-table** [**dot1p-dot1p** | **dot1p-dscp** | **dscp-dot1p** | **dscp-dscp**]，查看当前的各优先级间的映射关系。
  - 在AR1200系列、AR2240C、AR2204或AR2220L&AR2220E上，执行命令**display qos map-table** [**dot1p-dot1p** | **dot1p-dscp** | **dscp-dot1p** | **dscp-dscp** | **exp-exp**]，查看当前的各优先级间的映射关系。
  - 在AR2201-48FE、AR2204-24GE、AR2204-27GE、AR2204-27GE-P、AR2204-48GE-P、AR2204-51GE-P、AR2204-51GE、AR2204-51GE-R、AR2204E、AR2204E-D、AR2202-48FE、AR2220、AR2240或AR3200&AR3600系列上，执行命令**display qos map-table** [**dot1p-dot1p** | **dot1p-dscp** | **dot1p-lp** | **dscp-dot1p** | **dscp-dscp** | **dscp-lp** | **exp-exp** | **exp-lp**]，查看当前的各优先级间的映射关系。

----结束

2.6 配置举例

通过示例介绍如何应用优先级映射。配置示例中包括组网需求、配置注意事项、配置思路等。

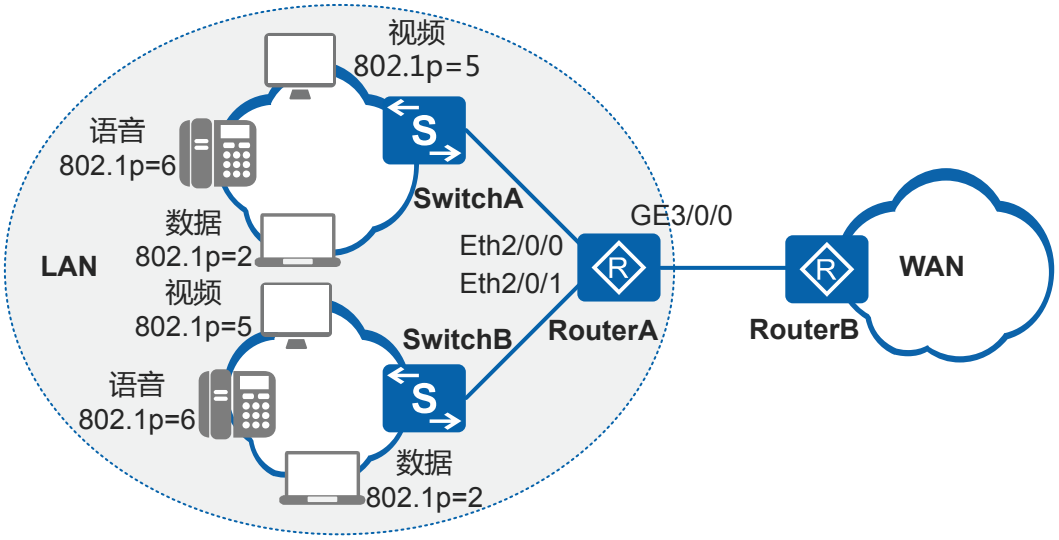
2.6.1 配置优先级映射示例

组网需求

如图2-5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Eth2/0/0和Eth2/0/1上，并通过RouterA的GE3/0/0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GE3/0/0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 2-5 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。

操作步骤

步骤1 创建VLAN并配置各接口

在RouterA上创建VLAN20和VLAN30。

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

配置接口Eth2/0/0和Eth2/0/1为Trunk类型端口，并将Eth2/0/0加入VLAN20，将Eth2/0/1加入VLAN30。

```
[RouterA] interface ethernet 2/0/0
[RouterA-Ethernet2/0/0] port link-type trunk
[RouterA-Ethernet2/0/0] port trunk allow-pass vlan 20
[RouterA-Ethernet2/0/0] quit
[RouterA] interface ethernet 2/0/1
[RouterA-Ethernet2/0/1] port link-type trunk
[RouterA-Ethernet2/0/1] port trunk allow-pass vlan 30
[RouterA-Ethernet2/0/1] quit
```

配置SwitchA与RouterA对接的接口为Trunk类型接口，并加入VLAN20。配置SwitchB与RouterA对接的接口为Trunk类型接口，并加入VLAN30。配置略。

创建VLANIF20和VLANIF30，并为VLANIF20配置IP地址192.168.2.1/24，为VLANIF30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GE3/0/0的IP地址为192.168.4.1/24。

```
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] ip address 192.168.4.1 24
[RouterA-GigabitEthernet3/0/0] quit
```

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Eth2/0/0和Eth2/0/1接口信任报文的802.1p优先级。

```
[RouterA] interface ethernet 2/0/0
[RouterA-Ethernet2/0/0] trust 8021p override
[RouterA-Ethernet2/0/0] quit
[RouterA] interface ethernet 2/0/1
[RouterA-Ethernet2/0/1] trust 8021p override
[RouterA-Ethernet2/0/1] 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> display current-configuration interface ethernet 2/0/0
#
interface Ethernet2/0/0
```

```
 port link-type trunk
 port trunk allow-pass vlan 20
 trust 8021p override
#
return
<RouterA> display current-configuration interface ethernet 2/0/1
#
interface Ethernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 30
 trust 8021p override
#
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 Ethernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 20
 trust 8021p override
#
interface Ethernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 30
 trust 8021p override
#
interface GigabitEthernet3/0/0
 ip address 192.168.4.1 255.255.255.0
#
return
```

2.7 常见配置错误

介绍优先级映射配置的常见错误。

2.7.1 报文未进入正确队列

常见原因

报文未进入正确队列的常见原因主要包括：

- 报文携带的优先级类型与入接口信任的优先级类型不一致。
- 优先级映射表中的优先级映射关系与要求不一致。

- 入接口有影响报文入队列的配置。

操作步骤

步骤1 检查入接口信任的优先级类型是否与报文携带的一致

进入接口视图，执行命令**display this**，查看入接口配置的**trust**命令（如果没有配置，则系统缺省不信任任何优先级），然后抓取入接口的报文，分析其携带的优先级类型并与接口信任的优先级类型进行比较：

说明

如果没有配置**trust**，设备按照**port priority**命令所配置的端口优先级入队列，这将导致所有报文进入同一队列，无法提供差分服务。

- 如果入接口信任的优先级类型与报文携带的不一致，执行命令**trust**修改入接口信任的优先级类型，使其与报文携带的优先级一致。
- 如果入接口信任的优先级类型与报文携带的一致，执行步骤2。

步骤2 检查优先级映射关系是否正确

- AR100&AR120&AR150&AR160&AR200系列、AR1200系列、AR2240C、AR2204或AR2220L&AR2220E按照802.1p优先级入队列，因此，需要查看入接口所信任的报文优先级(如DSCP、802.1p)到802.1p优先级的映射关系。
- AR2201-48FE、AR2204-24GE、AR2204-27GE、AR2204-27GE-P、AR2204-48GE-P、AR2204-51GE-P、AR2204-51GE、AR2204-51GE-R、AR2204E、AR2204E-D、AR2202-48FE、AR2220、AR2240或AR3200&AR3600系列按照内部优先级入队列，因此，需要查看入接口所信任的报文优先级(如DSCP、802.1p)到内部优先级的映射关系。

进入优先级映射表视图，执行命令**display this**检查优先级映射表中配置的优先级映射关系是否符合业务规划:

- 如果配置不符合业务规划，请执行命令**qos map-table**进入优先级映射表视图；然后执行命令**input**正确配置。
- 如果配置符合业务规划，请执行步骤3。

步骤3 检查入接口是否有影响报文入队列的配置

1. 检查入接口是否配置了带remark动作的流量监管

   进入接口视图，执行命令**display this**，查看接口上是否配置了带**remark-8021p**或**remark-dscp**参数的**qos car inbound**命令。

   - 如果配置了，请根据实际情况取消remark动作或执行命令**undo qos car inbound**取消配置的流量监管。
   - 如果没有配置，请执行步骤b。

2. 检查入接口是否配置了带remark动作的入方向的流策略

   进入接口视图，执行命令**display this**，查看接口上是否配置了**traffic-policy inbound**命令。

   - 如果配置了，则请执行命令**display traffic-policy applied-record** *policy-name*查看流策略的应用记录及其绑定的流行为，如果流策略应用**success**，请进一步执行命令**display traffic behavior user-defined**查看该流策略绑定的流行为里是否包含remark报文优先级（如**remark 8021p**、**remark dscp**）或**remark local-precedence**的动作。
     - 如果流策略绑定的流行为中配置了相应的remark动作，请根据需要取消流行为中的remark动作或者取消接口上的流策略配置。

- 如果流策略应用失败或者流策略绑定的流行为中没有配置remark动作，请执行步骤c。

- 如果没有配置，请执行步骤c。

3. 检查入接口是否配置了带入队列动作的出方向的流策略

   进入接口视图，执行命令**display this**，查看接口上是否配置了**traffic-policy outbound**命令。

   - 如果配置了，请执行命令**display traffic-policy applied-record** *policy-name*查看流策略的应用记录及其绑定的流行为，如果流策略应用**success**，请进一步执行命令**display traffic behavior user-defined**查看该流策略绑定的流行为的配置信息里是否包含**Assured Forwarding**、**Expedited Forwarding**或**Flow based Weighted Fair Queueing**等关键字，如果有，表明该流行为中有入队列的动作，请根据需要取消流行为中的入队列动作或者取消接口上的流策略配置。

----结束

2.7.2 优先级映射结果不正确

常见原因

优先级映射结果不正确的常见原因主要包括：

- 入接口信任的优先级类型与要求不一致。
- 对于AR2201-48FE、AR2204-24GE、AR2204-27GE、AR2204-27GE-P、AR2204-48GE-P、AR2204-51GE-P、AR2204-51GE、AR2204-51GE-R、AR2204E、AR2204E-D、AR2202-48FE、AR2220、AR2240或AR3200&AR3600系列设备，报文入接口配置的**trust**没有带**override**属性。
- 优先级映射表中配置的优先级映射关系与要求不一致。
- 报文入接口有影响优先级映射的配置。
- 报文出接口有影响优先级映射的配置。

操作步骤

步骤1 检查入接口信任的优先级类型是否正确

进入接口视图，执行命令**display this**，查看入接口配置的**trust**命令（如果没有配置，则系统缺省不信任任何优先级），确认信任的优先级类型是否与报文携带的优先级一致：

说明

- 对于AR100&AR120&AR150&AR160&AR200系列、AR1200系列、AR2240C、AR2204或AR2220L&AR2220E，如果没有配置**trust**或者报文携带的优先级与入接口信任的优先级不一致，设备按照**port priority**命令所配置的端口优先级查找802.1p优先级到各优先级映射表，修改报文的优先级。
- 对于AR2201-48FE、AR2204-24GE、AR2204-27GE、AR2204-27GE-P、AR2204-48GE-P、AR2204-51GE-P、AR2204-51GE、AR2204-51GE-R、AR2204E、AR2204E-D、AR2202-48FE、AR2220、AR2240或AR3200&AR3600系列，如果配置了**trust**，但报文携带的优先级与入接口信任的优先级不一致，此时若配置了**override**属性，设备按照**port priority**命令所配置的端口优先级查找802.1p优先级到各优先级映射表，修改报文的优先级。

- 如果报文携带的优先级与入接口信任的优先级不一致，执行命令**trust**正确配置入接口信任的优先级类型。

- 对于AR100&AR120&AR150&AR160&AR200系列、AR1200系列、AR2240C、AR2204或AR2220L设备，如果报文携带的优先级与入接口信任的优先级不一致，执行步骤3。
- 对于AR2201-48FE、AR2204-24GE、AR2204-27GE、AR2204-27GE-P、AR2204-48GE-P、AR2204-51GE-P、AR2204-51GE、AR2204-51GE-R、AR2204E、AR2204E-D、AR2202-48FE、AR2220、AR2240或AR3200&AR3600系列设备，如果报文携带的优先级与入接口信任的优先级一致，请执行步骤2。

步骤2 在AR2201-48FE、AR2204-24GE、AR2204-27GE、AR2204-27GE-P、AR2204-48GE-P、AR2204-51GE-P、AR2204-51GE、AR2204-51GE-R、AR2204E、AR2204E-D、AR2202-48FE、AR2220、AR2240或AR3200&AR3600系列上检查**trust**命令是否带了**override**属性

- 如果没有带**override**属性，则设备按照指定优先级映射后，并不修改报文的优先级，需要修改为带有**override**属性。
- 如果已带**override**属性，请执行步骤3。

步骤3 检查优先级映射关系是否正确

进入优先级映射表视图，执行命令**display this**检查优先级映射表中配置的优先级映射关系是否符合业务规划:

- 如果配置不符合业务规划，请执行命令**qos map-table**进入优先级映射表视图；然后执行命令**input**正确配置。
- 如果配置符合业务规划，请执行步骤4。

步骤4 检查报文入接口是否有影响优先级映射的配置

1. 检查报文入接口是否配置了带**remark**参数的基于接口的流量监管

   由于基于接口的流量监管的优先级高于优先级映射，如果入接口配置了带**remark-8021p**或**remark-dscp**参数的基于接口的流量监管，设备按照流量监管中**remark**后的优先级标记报文。

   进入接口视图，执行命令**display this**，查看接口上是否配置了带**remark-8021p**或**remark-dscp**参数的**qos car inbound**命令。

   - 如果配置了，请根据实际情况取消**remark**动作或执行命令**undo qos car inbound**取消配置的流量监管。
   - 如果没有配置，请执行步骤b。

2. 检查报文入接口是否配置了带**remark**动作的入方向的流策略

   由于流策略的优先级高于优先级映射，如果入接口配置了带**remark**报文优先级、**remark local-precedence**，或带**remark-8021p**或**remark-dscp**参数的**car**等动作的流策略，设备按照流策略中**remark**后的优先级标记匹配流分类的报文。

   进入接口视图，执行命令**display this**，查看接口上是否配置了**traffic-policy inbound**命令。

   - 如果配置了，则请执行命令**display traffic-policy applied-record** *policy-name*，查看流策略的应用记录及其绑定的流行为。

     如果流策略应用**success**，请进一步执行命令**display traffic behavior user-defined**查看该流策略绑定的流行为里是否包含**remark**报文优先级、**remark**内部优先级，或者带**remark-8021p**或**remark-dscp**参数的**car**等动作。

     - 如果流策略绑定的流行为中配置了上述动作，请根据需要取消流行为中的相应动作或者取消接口上的流策略配置。

- 如果流策略应用**fail**或者流策略绑定的流行为中没有配置上述动作，请执行步骤5。

- 如果没有配置，请执行步骤5。

步骤5 检查报文出接口是否有影响优先级映射的配置

1. 检查报文出接口是否配置了带**remark**参数的基于接口的流量监管

   由于基于接口的流量监管的优先级高于优先级映射，如果出接口配置了带**remark-8021p**或**remark-dscp**参数的基于接口的流量监管，设备按照流量监管中**remark**后的优先级标记报文。

   进入接口视图，执行命令**display this**，查看接口上是否配置了带**remark-8021p**或**remark-dscp**参数的**qos car outbound**命令。

   - 如果配置了，请根据实际情况取消**remark**动作或执行命令**undo qos car outbound**取消配置的流量监管。
   - 如果没有配置，请执行步骤b。

2. 检查报文出接口是否配置了带**remark**动作的出方向的流策略

   由于流策略的优先级高于优先级映射，如果出接口配置了带**remark**报文优先级、**remark local-precedence**，或带**remark-8021p**或**remark-dscp**参数的**car**等动作的流策略，设备按照流策略中**remark**后的优先级标记匹配流分类的报文。

   进入出接口视图，执行命令**display this**，查看接口上是否配置了**traffic-policy outbound**命令。如果配置了，则请执行命令**display traffic-policy applied-record** *policy-name*查看流策略的应用记录及其绑定的流行为。

   如果流策略应用**success**，请进一步执行命令**display traffic behavior user-defined**，查看该流策略绑定的流行为里是否包含**remark**报文优先级、**remark**内部优先级，或者带**remark-8021p**或**remark-dscp**参数的**car**等动作。如果流策略绑定的流行为中配置了上述动作，请根据需要取消流行为中的该动作或者取消接口上的流策略配置。

----结束

2.8 FAQ

介绍配置优先级映射的FAQ。

2.8.1 端口优先级有何用途

port priority命令用来设置端口优先级，即指定该端口入报文默认的优先级。AR根据优先级将报文送入不同的队列。缺省情况下，AR接口不信任报文优先级，报文按照端口优先级入队列。

如果接口下所有报文都按端口优先级入队列，必然导致所有报文进入同一队列，无法提供差分服务。使用**trust**命令指定对报文按照其自身携带的某类优先级进行优先级映射（即根据某类优先级查优先级映射表），然后：

- 对于AR100&AR120&AR150&AR160&AR200和AR1200系列，设备按照映射后的802.1p优先级将报文送入不同的端口队列，进而通过队列调度，为不同优先级的报文提供相应的服务。
- 对于AR2200系列，

- 从V200R001C00版本开始，设备按照映射后的802.1p优先级将报文送入不同的端口队列，进而通过队列调度，为不同优先级的报文提供相应的服务。
- 从V200R003C00版本开始，AR2204、AR2220L和AR2220E按照映射后的802.1p优先级将报文送入不同的端口队列，进而通过队列调度，为不同优先级的报文提供相应的服务；AR2201、AR2202、AR2220、AR2240C和AR2240按照映射后的本地优先级将报文送入不同的端口队列，进而通过队列调度，为不同优先级的报文提供相应的服务。

- 对于AR3200&AR3600系列，设备按照映射后的本地优先级将报文送入不同的端口队列，进而通过队列调度，为不同优先级的报文提供相应的服务。

2.8.2 AR100&AR120&AR150&AR160&AR200 系列、AR1200 的 Trust 命令和 AR2200 系列、AR3200&AR3600 系列的 Trust 命令有什么不同

- V200R001C00版本：
  - AR1200系列的**trust**命令不可配置**override**关键字，默认修改报文中的优先级字段；
  - AR2200&AR3200&AR3600系列的**trust**命令，可配置**override**字段，用户可以自由选择是否修改报文中优先级字段。
- 从V200R001C01版本开始：
  - AR1200的**trust**命令未配置**override**关键字时，报文按照指定优先级映射后，报文的802.1p值被修改成映射后的值，报文的DSCP值保持不变；配置**override**关键字时，报文按照指定优先级映射后，报文的802.1p值、DSCP值均被修改成映射后的值。
  - AR2200&AR3200&AR3600系列的**trust**命令，可配置**override**字段，用户可以自由选择是否修改报文中优先级字段。
- 从V200R002C00版本开始：
  - AR100&AR120&AR150&AR160&AR200系列和AR1200的**trust**命令未配置**override**关键字时，报文按照指定优先级映射后，报文的802.1p值被修改成映射后的值，报文的DSCP值保持不变；配置**override**关键字时，报文按照指定优先级映射后，报文的802.1p值、DSCP值均被修改成映射后的值。
  - AR2200&AR3200&AR3600系列的**trust**命令，可配置**override**字段，用户可以自由选择是否修改报文中优先级字段。
- 从V200R003C00版本开始：
  - AR100&AR120&AR150&AR160&AR200系列、AR1200系列、AR2204、AR2220L和AR2220E的**trust**命令未配置**override**关键字时，报文按照指定优先级映射后，报文的802.1p值被修改成映射后的值，报文的DSCP值保持不变；配置**override**关键字时，报文按照指定优先级映射后，报文的802.1p值、DSCP值均被修改成映射后的值。
  - AR2201&AR2202&AR2220&AR2240C&AR2240&AR3200&AR3600系列的**trust**命令，可配置**override**字段，用户可以自由选择是否修改报文中优先级字段。

2.9 参考信息

介绍QoS特性的相关参考资料。

文档	描述	备注
RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	-
RFC 2475	An Architecture for Differentiated Services	-
RFC 2597	Assured Forwarding PHB Group	-
RFC 2598	An Expedited Forwarding PHB	-
RFC 2697	A Single Rate Three Color Marker	-
RFC 2698	A Two Rate Three Color Marker	-

3 流量监管和流量整形配置

关于本章

流量监管和流量整形配置介绍了流量监管和流量整形基本概念，并介绍了基于流的流量监管、配置流量整形的配置方法和配置示例。

3.1 流量监管和流量整形概述
流量监管和流量整形通过监督进入网络的流量速率，用来限制流量及其资源的使用，保证更好的为用户提供服务。

3.2 原理描述
介绍令牌桶与流量评估的基本原则，以及流量监管，流量整形和接口限速的实现原理。

3.3 应用场景
介绍流量监管、流量整形和接口限速的应用场景。

3.4 缺省配置
介绍流量监管和流量整形的缺省配值，实际应用的配置可以基于缺省配置进行修改。

3.5 配置流量监管
配置基于接口的流量监管后，设备将对接口上所有的业务流量进行流量监管；配置基于流的流量监管后，设备将对符合流分类规则的报文进行流量监管。

3.6 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。

3.7 配置物理接口限速
WAN侧物理接口支持接口限速功能，通过配置接口发送报文速率占接口带宽的百分比，实现对接口发送报文速率的限制。

3.8 维护流量监管和流量整形
流量监管和流量整形的维护，包括查看流量统计信息、清除流量统计数据。

3.9 配置举例
通过示例介绍配置流量监管和流量整形。配置示例中包括组网需求、配置注意事项、配置思路等。

3.10 FAQ

介绍配置流量监管和流量整形的FAQ。

3.11 参考信息

3.1 流量监管和流量整形概述

流量监管和流量整形通过监督进入网络的流量速率，用来限制流量及其资源的使用，保证更好的为用户提供服务。

如果报文的发送速率大于接收速率，或者下游设备的接口速率小于上游设备的接口速率，就会引起网络拥塞。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。

流量监管和流量整形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策略。

流量监管

流量监管TP（Traffic Policing）就是对流量进行控制，通过监督进入网络的流量速率，对超出部分的流量进行“惩罚”，使进入的流量被限制在一个合理的范围之内，从而保护网络资源和用户的利益。

流量整形

流量整形TS（Traffic Shaping）是一种主动调整流量输出速率的措施。当下游设备的入接口速率小于上游设备的出接口速率或发生突发流量时，下游设备入接口处可能出现流量拥塞的情况，此时用户可以通过在上游设备的接口出方向配置流量整形，将上游不规整的流量进行削峰填谷，输出一条比较平整的流量，从而解决下游设备的拥塞问题。

流量整形与流量监管的主要区别在于，流量整形对原本要被丢弃的报文进行缓存，当令牌桶有足够的令牌时，再均匀的向外发送这些被缓存的报文。流量整形与流量监管的另一区别是，整形可能会增加延迟，而监管几乎不引入额外的延迟。

相关资料

视频：**AR G3系列路由器QOS特性介绍**

3.2 原理描述

介绍令牌桶与流量评估的基本原则，以及流量监管，流量整形和接口限速的实现原理。

网络中存在不同用户的多种业务流量，如果对所有用户的业务流量都不加限制，那么当大量用户产生不断突发的业务数据时，网络会更加拥挤。为了使有限的网络资源能够更好地发挥效用，更好地为更多的用户服务，必须对用户的业务流量加以限制。

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

3.2.1 令牌桶技术

概述

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

在使用令牌桶对流量进行评估时，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，否则称为流量超标或不符合约定值。

关于令牌桶处理报文的方式，RFC中定义了两种标记算法：

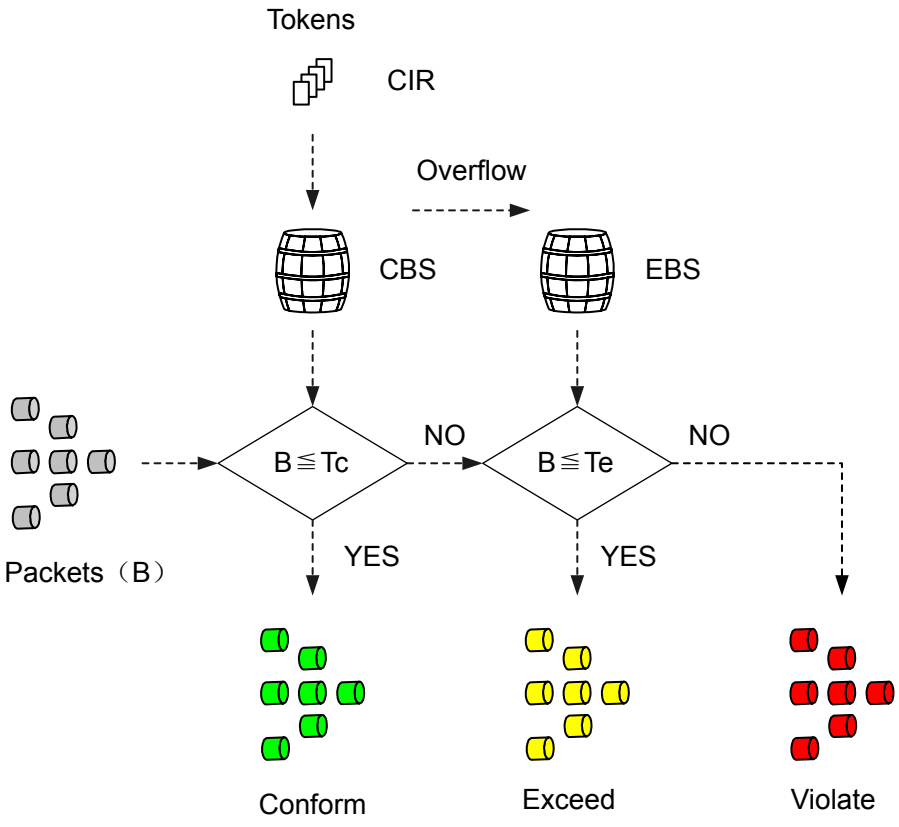
- 单速率三色标记（single rate three color marker，srTCM，或称为单速双桶算法）算法，主要关注报文尺寸的突发。
- 双速率三色标记（two rate three color marker，trTCM，或称为双速双桶算法）算法，主要关注报文速率的突发。

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

单速双桶

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

图 3-1 单速双桶示意图



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

- CIR：承诺信息速率，表示向C桶中投放令牌的速率，即C桶允许传输或转发报文的平均速率；
- CBS：承诺突发尺寸，表示C桶的容量，即C桶瞬间能够通过的承诺突发流量；
- EBS（Excess Burst Size）：超额突发尺寸，表示E桶的容量，即E桶瞬间能够通过的超出突发流量。

系统按照CIR速率向桶中投放令牌：

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

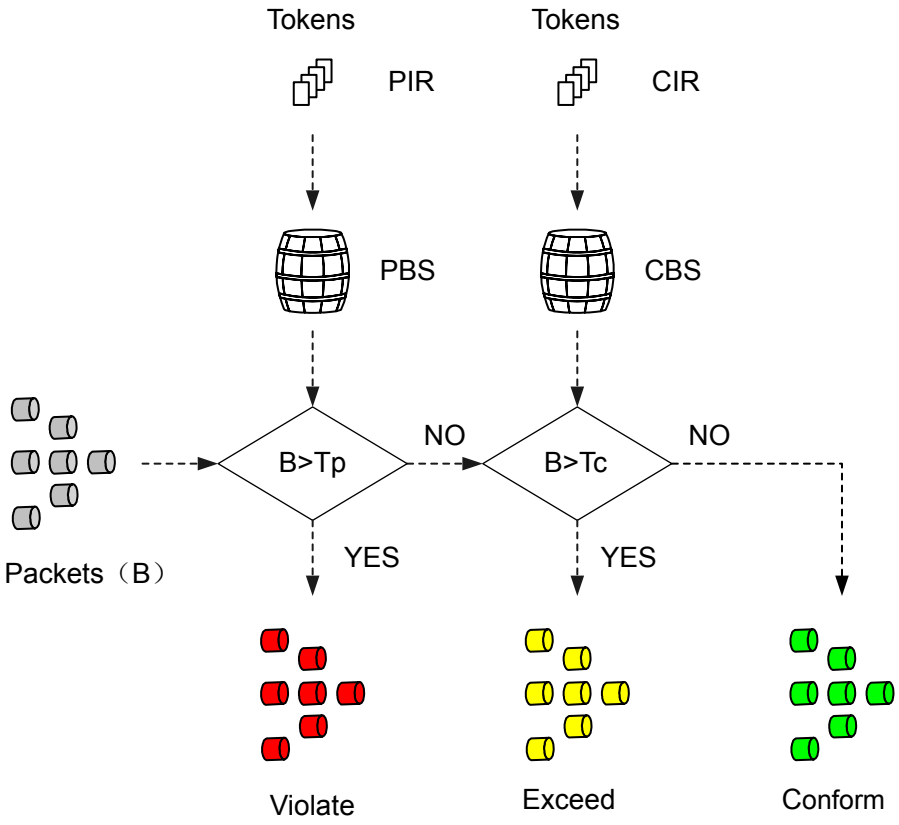
对于到达的报文，用B表示报文的大小：

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

双速双桶

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

图 3-2 双速双桶示意图



如图3-2所示，为方便描述将两个令牌桶称为P桶和C桶，用Tp和Tc表示桶中的令牌数量。双速双桶有4个参数：

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

系统按照PIR速率向P桶中投放令牌，按照CIR速率向C桶中投放令牌：

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

对于到达的报文，用B表示报文的大小：

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

色敏模式

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

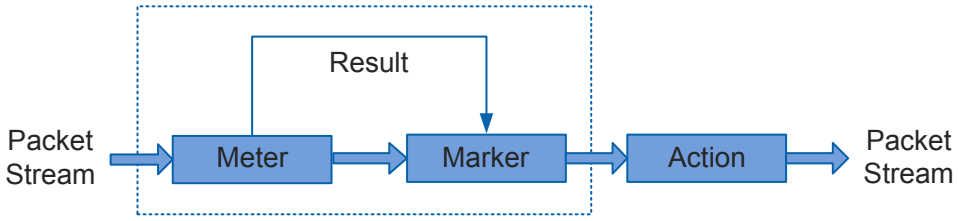
- 如果报文已被标记为绿色，则令牌桶的评估机制与色盲模式保持一致。
- 如果报文已被标记为黄色，则令牌桶根据报文长度和令牌数的大小，为符合流量规定的报文标记为黄色，为不符合的报文标记为红色。
- 如果报文已被标记为红色，则令牌桶直接将到达报文标记为红色。

3.2.2 流量监管

流量监管就是对流量进行控制，通过监督进入网络的流量速率，对超出部分的流量进行“惩罚”，使进入的流量被限制在一个合理的范围之内，从而保护网络资源和企业网用户的利益。

流量监管的原理

图 3-3 流量监管组件



如图3-3所示，流量监管由三部分组成：

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

  默认情况下，green报文、yellow报文进行转发，red报文丢弃。

经过流量监管，如果某流量速率超过标准，设备可以选择降低报文优先级再进行转发或者直接丢弃。默认情况下，此类报文被丢弃。

3.2.3 流量整形

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

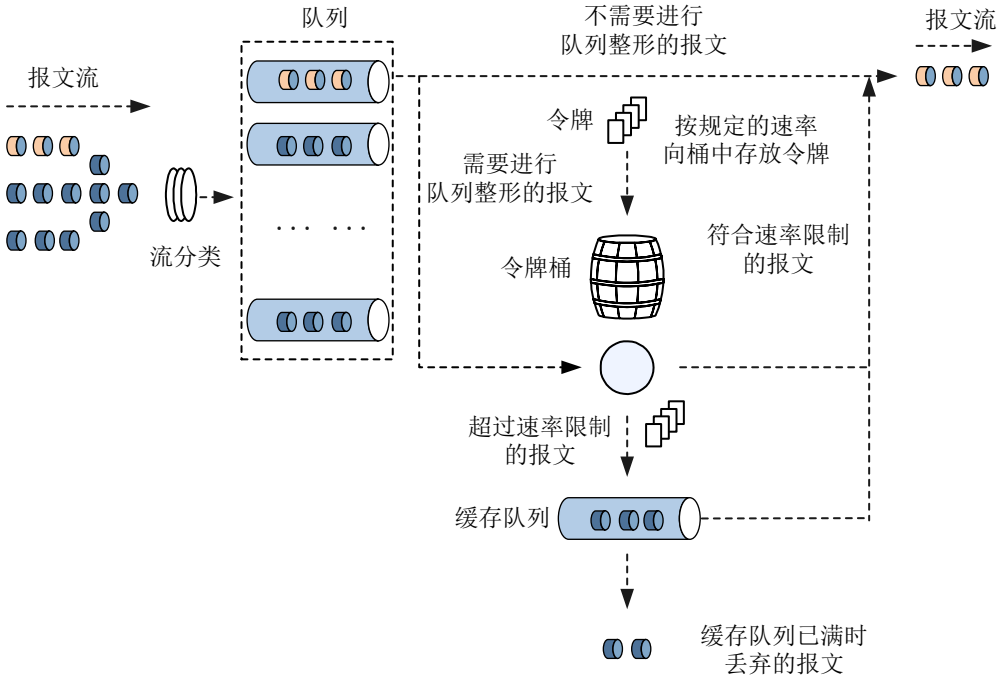
当下游设备的接口速率小于上游设备的接口速率或发生突发流量，在下游设备接口处可能出现流量拥塞的情况，此时用户可以通过在上游设备的接口出方向配置流量整形，将上游不规整的流量进行削峰填谷，输出一条比较平整的流量，从而解决下游设备的拥塞问题。

处理流程

流量整形是一种应用于接口、子接口或队列的流量控制技术，可以对从接口上经过的所有报文或某类报文进行速率限制。

下面以接口或子接口下采用单速单桶技术的基于流的队列整形为例介绍流量整形的处理流程，其处理流程如图3-4所示。

图 3-4 流量整形处理流程图



具体处理流程如下：

1. 当报文到来的时候，首先对报文进行分类，使报文进入不同的队列。
2. 若报文进入的队列没有配置队列整形功能，则直接发送该队列的报文；否则，进入下一步处理。
3. 按用户设定的队列整形速率向令牌桶中放置令牌：
   - 如果令牌桶中有足够的令牌可以用来发送报文，则报文直接被发送，在报文被发送的同时，令牌做相应的减少。
   - 如果令牌桶中没有足够的令牌，则将报文放入缓存队列，如果报文放入缓存队列时，缓存队列已满，则丢弃报文。
4. 缓存队列中有报文的时候，系统按一定的周期从缓存队列中取出报文进行发送，每次发送都会与令牌桶中的令牌数作比较，直到令牌桶中的令牌数减少到缓存队列中的报文不能再发送或缓存队列中的报文全部发送完毕为止。

队列整形后，如果该接口和子接口同时配置了接口整形，则系统还要逐级按照子接口整形速率、接口整形速率对报文流进行速率控制。其处理流程与队列整形相似，但不需要步骤1和步骤2。

自适应流量整形

流量整形主要是为了解决下游设备的接口速率小于上游设备的接口速率，从而导致下游设备接口入方向丢包的问题。但有些场景下，下游设备的接口速率是不确定的，上游设备无法确定应该把整形参数设置为多少。此时可以配置自适应模板来实现自适应流量整形，通过在上游设备和下游设备间开启NQA检测，根据NQA检测到的下游设备丢包率动态调整整形参数。

自适应模板规定了：

- NQA测试例：通过此测试例检测下游设备接口入方向丢包率，根据检测结果调整整形参数。
- 整形速率范围：上游设备接口出方向的整形速率上下限，整形速率在此范围内动态调整。
- 整形速率调整步长：动态调整整形速率时，每次调整的速率大小。
- 丢包率范围：下游设备接口入方向允许的丢包率范围。当丢包率在此范围之内时，不调整整形速率；当丢包率过大，减小上游设备整形速率；当丢包率过小，且上游设备发生拥塞，增大上游设备整形速率。
- 整形速率增大的时间间隔：当丢包率在阈值附近频繁变化时，就需要频繁调整整形速率，用户可以通过设置此参数，限制增大整形速率的时间间隔，避免频繁更新。

  说明

  当NQA检测到丢包率过大，为避免业务数据进一步丢失，立即减小整形速率，不需要满足时间间隔的要求。

系统根据NQA检测结果中的丢包率等调整整形速率：

触发条件（必须同时满足所有条件）	动作
NQA检测到丢包率大于自适应模板配置的丢包率上限	减小整形速率
● NQA检测到丢包率小于自适应模板配置的丢包率下限 ● 上游发送端接口拥塞 ● 距离上次增大整形速率的时间间隔超过自适应模板配置的速率增大时间间隔	增大整形速率
● NQA检测到丢包率小于自适应模板配置的丢包率下限 ● 上游发送端接口不拥塞	保持当前整形速率
丢包率在自适应模板配置的丢包率范围内	保持当前整形速率
检测失败	自适应模板配置的整形速率上限

说明

若自适应模板未绑定NQA测试例，则整形速率取自适应模板配置的整形速率上限。

3.3 应用场景

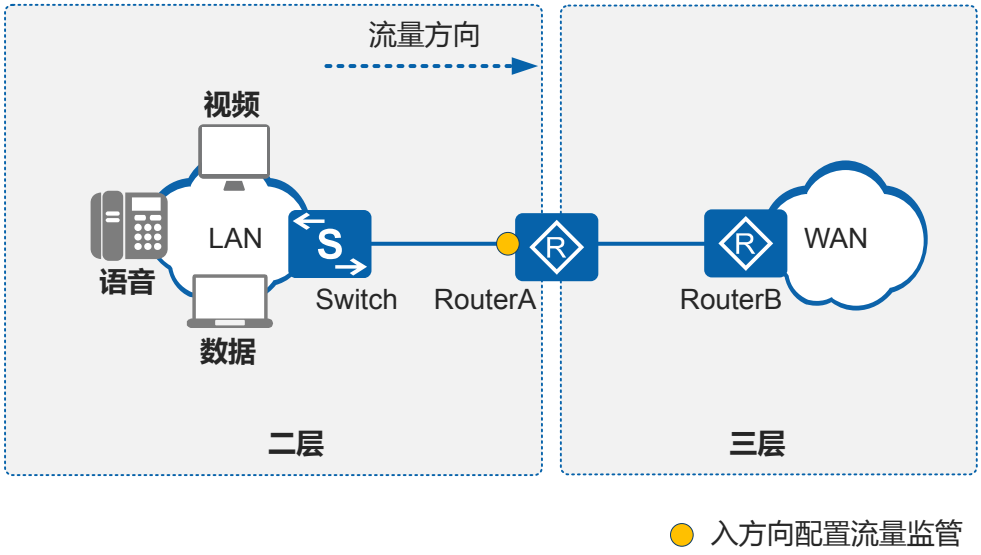
介绍流量监管、流量整形和接口限速的应用场景。

流量监管的应用

在企业网络中，存在语音、视频和数据等多种不同的业务，当大量的业务流量进入网络侧时，可能会因为带宽不足产生拥塞，需要对三种业务提供不同的保证带宽，优先

保证语音业务的带宽，其次是视频业务，最后是数据业务，因此可以对不同业务进行不同的流量监督，为语音报文提供最大保证带宽，视频报文次之，数据报文保证带宽最小，从而在网络产生拥塞时，可以保证语音报文优先通过。如图3-5所示。

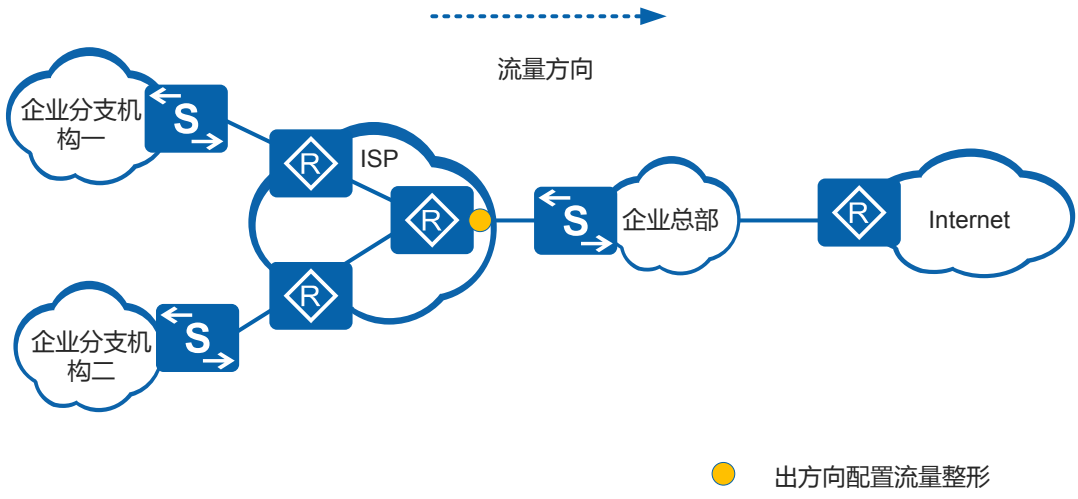
图 3-5 流量监管应用组网图



流量整形的应用

企业网络中，总部与分支机构通过ISP网络使用专线相连。分支机构想要访问Internet必须通过总部。如果所有分支机构同时访问Internet，可能导致访问Internet的Web流量产生拥塞，从而被丢弃。如图3-6所示，为了防止Web流量的丢失，可以在企业分支机构的流量进入企业总部之前配置流量整形。

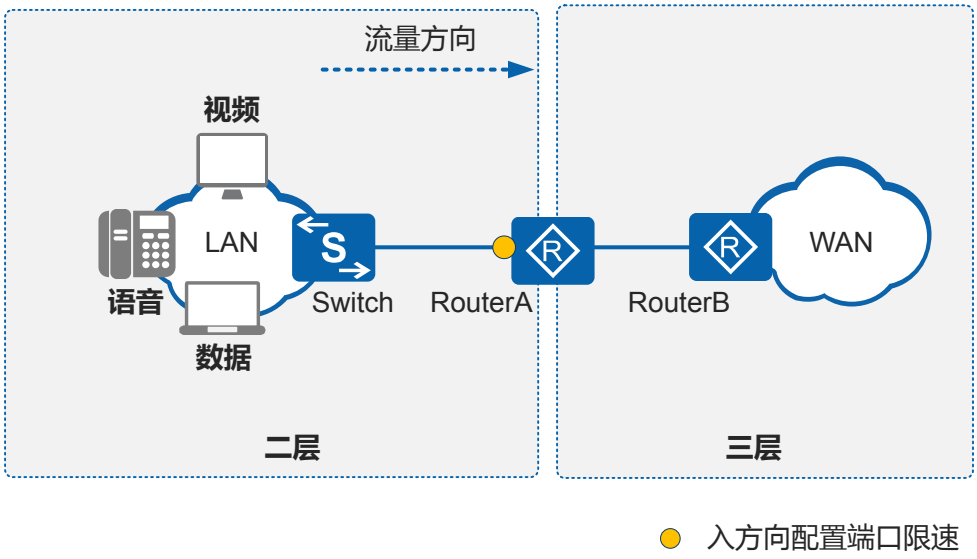
图 3-6 流量整形应用组网图



接口限速的应用

在企业网络中，当大量的业务流量进入网络侧时，可能会因为带宽不足产生拥塞，需要对进入网络侧的流量进行限制，可以在路由器的入接口上配置接口限速，将进入网络侧的流量限制在规定范围内，超出的流量将被丢弃。如图3-7所示。

图 3-7 接口限速应用组网图



3.4 缺省配置

介绍流量监管和流量整形的缺省配值，实际应用的配置可以基于缺省配置进行修改。

流量监管的缺省配值如表3-1所示，流量整形的缺省配值如表3-2所示。

表 3-1 流量监管的缺省配值

参数	缺省值
基于接口的流量监管	未对接口进行流量监管
基于流的流量监管	未对不同的业务流进行流量监管

表 3-2 流量整形的缺省配值

参数	缺省值
基于接口的流量整形	未对接口进行流量整形

3.5 配置流量监管

配置基于接口的流量监管后，设备将对接口上所有的业务流量进行流量监管；配置基于流的流量监管后，设备将对符合流分类规则的报文进行流量监管。

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。

3.5.1 配置基于接口的流量监管

背景信息

若需要对接口出/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。

说明

AR100&AR120系列、AR161、AR161W、AR169、AR161G-L、AR161G-Lc、AR161EW、AR161EW-M1、AR161G-U、AR169G-L、AR169EW、AR169CVW、AR169CVW-4B4S、AR169EGW-L、AR169W-P-M9、AR169RW-P-M9、AR169-P-M9、AR1220E、AR1220EV和AR1220EVW的LAN侧接口都不支持基于接口的流量监管。

4GE-2S单板不支持基于接口的流量监管。

V200R008C50及以后版本，二层VE接口支持WAN侧流量监管命令。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 （可选）执行命令**qos overhead layer** { **link** | **physics** }，配置在流量监管或流量整形时报文长度的计算方式。

缺省情况下，流量监管或流量整形计算报文长度时包括报文的物理层和链路层的补偿信息。

步骤3 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4 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。

说明

V200R008C50及以后版本，二层VE接口仅支持WAN侧流量监管命令。

- 配置WAN接口的流量监管。
  - AR100&AR120&AR150&AR160&AR200系列：执行命令**qos car** { **inbound** | **outbound** } [**acl** *acl-number* | { **destination-ip-address** | **source-ip-address** } **range** *start-ip-address* **to** *end-ip-address* [**per-address**] [**time-range** *time-range-name*]] **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*] }]。

- AR100&AR120系列、AR161、AR161W、AR161G-L、AR161EW、AR161EW-M1、AR161G-Lc、AR161G-U、AR169、AR169G-L、AR169EGW-L、AR169-P-M9、AR169RW-P-M9、AR169W-P-M9：执行命令**qos car** { **inbound** | **outbound** } **user-set** *user-set-name* **cir** *cir-value* [**cbs** *cbs-value* **pbs** *pbs-value*] [**time-range** *time-range-name*] [**green** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] [**yellow** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] [**red** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }]。
- AR1200&AR2200&AR3200&AR3600系列：执行命令**qos car** { **inbound** | **outbound** } [**acl** *acl-number* | { **destination-ip-address** | **source-ip-address** } **range** *start-ip-address* **to** *end-ip-address* [**per-address**] [**time-range** *time-range-name*]] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] [**yellow** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] [**red** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }]。

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*或配置*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*且配置*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。

- 配置LAN接口的流量监管。
  - 执行命令**qos car inbound cir** *cir-value*，配置接口下所有业务流量的流量监管。
  - AR100&AR120&AR150&AR160&AR200系列：执行命令**qos car** { **inbound** | **outbound** } { **acl** *acl-number* | { **destination-ip-address** | **source-ip-address** } **range** *start-ip-address* **to** *end-ip-address* [**per-address**] [**time-range** *time-range-name*] } **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*] }]。

    说明

    AR161、AR161W、AR169、AR169EW、AR169CVW、AR169CVW-4B4S、AR169EGW-L、AR161G-L、AR161EW、AR161EW-M1、AR161G-Lc、AR161G-U、AR169G-L、AR169W-P-M9、AR169RW-P-M9和AR169-P-M9不支持对接口下所有业务流量进行流量监管，支持对符合指定ACL规则或对源、目的IP属于指定范围的业务流量进行流量监管。
  - AR1200&AR2200&AR3200&AR3600系列：执行命令**qos car** { **inbound** | **outbound** } { **acl** *acl-number* | { **destination-ip-address** | **source-ip-address** } **range** *start-ip-address* **to** *end-ip-address* [**per-address**] [**time-range** *time-range-name*] } **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] [**yellow** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] [**red** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }]。

说明

AR1220E、AR1220EV和AR1220EVW不支持对接口下所有业务流量进行流量监管，支持对符合指定ACL规则或对源、目的IP属于指定范围的业务流量进行流量监管。

----结束

3.5.2 配置 MQC 实现流量监管

背景信息

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

操作步骤

1. 配置流分类
   a. 执行命令**system-view**，进入系统视图。
   b. 执行命令**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]，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”，指定该逻辑关系后：
      - 当流分类中有ACL规则时，报文必须匹配其中一条ACL规则以及所有非ACL规则才属于该类。
      - 当流分类中没有ACL规则时，则报文必须匹配所有非ACL规则才属于该类。

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

      缺省情况下，流分类中各规则之间的关系为“逻辑或”。
   c. 请根据实际情况配置流分类中的匹配规则。

匹配规则	命令
外层VLAN ID	**if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*]
QinQ报文内层VLAN ID	**if-match cvlan-id** *start-vlan-id* [**to** *end-vlan-id*]
VLAN报文802.1p优先级	**if-match 8021p** *8021p-value* &<1-8>
QinQ报文内层VLAN的802.1p优先级	**if-match cvlan-8021p** *8021p-value* &<1-8>
MPLS报文EXP优先级（AR1200&AR2200&AR3200&AR3600系列）	**if-match mpls-exp** *exp-value* &<1-8>
目的MAC地址	**if-match destination-mac** *mac-address* [**mac-address-mask** *mac-address-mask*]

匹配规则	命令
源MAC地址	**if-match source-mac** *mac-address* [**mac-address-mask** *mac-address-mask*]
FR报文中的DLCI信息	**if-match dlci** *start-dlci-number* [**to** *end-dlci-number*]
FR报文中的DE标志位	**if-match fr-de**
以太网帧头中协议类型字段	**if-match l2-protocol** { **arp** | **ip** | **mpls** | **rarp** | *protocol-value* }
所有报文	**if-match any**
IP报文的DSCP优先级	**if-match** [**ipv6**] **dscp** *dscp-value* &<1-8> **说明** 如果流策略中配置了匹配DSCP，则SAE220（WSIC）和SAE550（XSIC）单板不支持**redirect ip-nexthop** *ip-address* **post-nat**动作。
IP报文的IP优先级	**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 [ipv6] dscp**和**if-match ip-precedence**。
报文三层协议类型	**if-match protocol** { **ip** | **ipv6** }
指定QoS group索引的IPSec报文	**if-match qos-group** *qos-group-value*
IPv4报文长度	**if-match packet-length** *min-length* [**to** *max-length*]
ATM报文中的PVC信息	**if-match pvc** *vpi-number*/*vci-number*
RTP端口号	**if-match rtp start-port** *start-port-number* **end-port** *end-port-number*
TCP报文SYN Flag	**if-match tcp syn-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** }*
入接口	**if-match inbound-interface** *interface-type interface-number*
出接口	**if-match outbound-interface Cellular** *interface-number:channel*
ACL规则	**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。 ● 当使用ACL作为流分类规则匹配源IP地址时，通过在接口下的**qos pre-nat**配置NAT预分类功能，可以将NAT转换前的私网IP地址信息携带到出接口，即可实现基于私网IP地址的分类，从而对来自不同私网IP地址的报文提供差分服务。

匹配规则	命令
ACL6规则	**if-match ipv6 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。 ● 当使用ACL作为流分类规则匹配源IP地址时，通过在接口下的**qos pre-nat**配置NAT预分类功能，可以将NAT转换前的私网IP地址信息携带到出接口，即可实现基于私网IP地址的分类，从而对来自不同私网IP地址的报文提供差分服务。
应用协议	**if-match application** *application-name* [**user-set** *user-set-name*] [**time-range** *time-name*] **说明** 定义基于应用协议的匹配规则前，必须使能SA功能并加载特征库。
SA协议组	**if-match category** *category-name* [**user-set** *user-set-name*] [**time-range** *time-name*] **说明** ● 定义基于应用协议的匹配规则前，必须使能SA功能并加载特征库。
用户组	**if-match user-set** *user-set-name* [**time-range** *time-range-name*]

d. 执行命令**quit**，退出流分类视图。

2. 配置流行为

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

b. 执行命令**car cir** { *cir-value* | **pct** *cir-percentage* } [**pir** { *pir-value* | **pct** *pir-percentage* }] [**cbs** *cbs-value* **pbs** *pbs-value*] [**share**] [**mode** { **color-blind** | **color-aware** }] [**green** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] [**yellow** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] [**red** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-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。

说明

- AR100&AR120&AR150&AR160&AR200系列不支持**remark-mpls-exp** *exp-value*参数。
- 对于Dialer接口，可以在Dialer接口视图下执行命令**bandwidth** *bandwidth-value*配置流行为CAR中的**pct** *cir-percentage*的基值，根据需要分配该接口基于MQC限速的各流量的百分比及实际限速带宽。

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

d. 执行命令**quit**，退出流行为视图。

e. （可选）执行命令**qos overhead layer** { **link** | **physics** }，配置在流量监管或流量整形时报文长度的计算方式。

缺省情况下，流量监管或流量整形计算报文长度时包括报文的物理层和链路层的补偿信息。

f. 执行命令**quit**，退出系统视图。

3. 配置流策略

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**traffic policy** *policy-name*，创建一个流策略并进入流策略视图，或进入已存在的流策略视图。

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

d. 执行命令**quit**，退出流策略视图。

e. 执行命令**quit**，退出系统视图。

4. 应用流策略

- 在接口下应用流策略

i. 执行命令**system-view**，进入系统视图。

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

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

- 在安全域间应用流策略

说明

仅AR100&AR120&AR150&AR160&AR200系列支持此步骤。

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**firewall interzone** *zone-name1 zone-name2*，创建安全域间并进入安全域间视图。

缺省情况下，未创建安全域间。

创建安全域间必须指定两个已存在的安全区域。

iii. 执行命令**traffic-policy** *policy-name*，在安全域间绑定流策略。

缺省情况下，安全域间没有绑定流策略。

- 在BD下应用流策略

说明

仅在V200R008C30及之后版本，AR100&AR120&AR150&AR160&AR200&AR1200系列和AR2220E支持此步骤。

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**bridge-domain** *bd-id*，创建广播域BD（Bridge Domain）并进入BD视图。

缺省情况下，没有创建广播域BD。

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

缺省情况下，BD下没有应用任何流策略。

3.5.3 检查配置结果

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 applied-record** [*policy-name*]，查看指定流策略的应用记录信息。
- 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* } { **inbound** | **outbound** }，查看接口上通过和丢弃报文的统计信息。

----结束

3.6 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。

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。

3.6.1 配置基于接口的流量整形

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 （可选）执行命令**qos overhead layer** { **link** | **physics** }，配置在流量监管或流量整形时报文长度的计算方式。

缺省情况下，流量监管或流量整形计算报文长度时包括报文的物理层和链路层的补偿信息。

步骤3 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4 执行命令**qos gts cir** *cir-value* [**cbs** *cbs-value*]，配置接口整形。

缺省情况下，不进行接口的流量整形。

说明

- AR100&AR120&AR150&AR160&AR200系列和AR1200系列面板上的二层接口不支持**qos gts**。
- 9ES2、4GE-2S、4ES2G-S和4ES2GP-S单板不支持**qos gts**。

----结束

3.6.2 配置基于接口的自适应流量整形

背景信息

若下游设备接口速率小于上游设备的接口速率，且下游设备接口速率不确定时，可以在上游设备配置基于接口的自适应流量整形，在一定程度上避免网络产生拥塞、丢包现象。

自适应流量整形可以通过在上游设备和下游设备间开启NQA检测，根据NQA检测到的下游设备丢包率动态调整整形参数：

- 当NQA检测到丢包率大于自适应模板配置的丢包率上限，则减小整形速率。
- 当NQA检测到丢包率小于自适应模板配置的丢包率下限，上游发送端接口拥塞，且距离上次增大整形速率的时间间隔超过自适应模板配置的速率增大时间间隔，则增大整形速率。
- 当NQA检测到丢包率小于自适应模板配置的丢包率下限，且上游发送端接口不拥塞，保持当前整形速率。
- 当NQA检测到丢包率在自适应模板配置的丢包率范围内，保持当前整形速率。
- 若NQA检测失败，则整形速率取自适应模板配置的整形速率上限。
- 若自适应模板未绑定NQA测试例，则整形速率取自适应模板配置的整形速率上限。

操作步骤

步骤1 配置自适应模板

1. 执行命令**system-view**，进入系统视图。
2. （可选）执行命令**qos overhead layer** { **link** | **physics** }，配置在流量监管或流量整形时报文长度的计算方式。

   缺省情况下，流量监管或流量整形计算报文长度时包括报文的物理层和链路层的补偿信息。
3. 执行命令**qos adaptation-profile** *adaptation-profile-name*，创建自适应模板，并进入自适应模板视图。
4. 执行命令**rate-range low-threshold** *low-threshold-value* **high-threshold** *high-threshold-value*，配置自适应模板的整形速率范围。
5. （可选）执行命令**rate-adjust step** *step*，配置自适应模板的整形速率调整步长。
6. （可选）执行命令**rate-adjust increase interval** *interval-value*，配置自适应模板中整形速率增大的时间间隔。
7. （可选）执行命令**rate-adjust loss low-threshold** *low-threshold-percentage* **high-threshold** *high-threshold-percentage*，配置自适应模板的丢包率范围。
8. 执行命令**track nqa** *admin-name test-name*，为自适应模板绑定NQA测试例。

说明

配置NQA测试例时，需保证NQA探测报文的优先级别，确保报文能够进入高优先级队列，不会在链路流量较大时被丢弃。

9. 执行命令**quit**，退出自适应模板视图。

步骤2 应用自适应模板

1. 执行命令**interface** *interface-type interface-number*[.*subinterface-number*]，进入接口视图或子接口视图。
2. 执行命令**qos gts adaptation-profile** *adaptation-profile-name*，在接口下应用自适应模板。

----结束

3.6.3 配置基于队列的流量整形

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。

说明

- AR100&AR120、AR161、AR161W、AR169、AR161G-L、AR161G-Lc、AR161EW、AR161EW-M1、AR161G-U、AR169G-L、AR169EW、AR169CVW、AR169CVW-4B4S、AR169EGW-L、AR169W-P-M9、AR169RW-P-M9、AR169-P-M9、AR1220E、AR1220EV、AR1220EVW、AR1220C、AR1220-8GE和AR1220F面板上的二层口不支持**qos queue-profile（接口视图）**。
- 9ES2、4GE-2S、4ES2G-S和4ES2GP-S单板不支持**qos queue-profile（接口视图）**。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 （可选）执行命令**qos overhead layer** { **link** | **physics** }，配置在流量监管或流量整形时报文长度的计算方式。

缺省情况下，流量监管或流量整形计算报文长度时包括报文的物理层和链路层的补偿信息。

步骤3 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4 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。

说明

4GE-2S、4ES2G-S、4ES2GP-S和9ES2单板上的接口不支持**queue length**配置。

AR150&200系列的二层FE接口不支持**queue length**配置。

AR100&AR120&AR160系列的二层GE接口不支持**queue length**配置。

AR1200系列主控板上FE接口不支持**queue length**配置。

步骤5 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。

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*]，进入需要配置队列整形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

3.6.4 配置 MQC 实现流量整形

背景信息

若需要对接口出方向的某类流量进行控制时，可以配置MQC实现流量整形，相同的流策略可以在不同的接口下应用，当匹配流分类规则的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。配置MQC实现流量整形，可以通过流分类，为不同业务提供更细致的差分服务。

说明

V200R008C30及以前版本，包含此流行为的流策略只能应用在设备的WAN接口出方向上。

V200R008C50及以后版本，包含此流行为的流策略可以应用在设备的WAN接口和二层VE接口出方向上。

操作步骤

1. 配置流分类
   a. 执行命令**system-view**，进入系统视图。
   b. 执行命令**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]，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”，指定该逻辑关系后：

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

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

      缺省情况下，流分类中各规则之间的关系为“逻辑或”。
   c. 请根据实际情况配置流分类中的匹配规则。

匹配规则	命令
外层VLAN ID	**if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*]
QinQ报文内层VLAN ID	**if-match cvlan-id** *start-vlan-id* [**to** *end-vlan-id*]
VLAN报文802.1p优先级	**if-match 8021p** *8021p-value* &<1-8>
QinQ报文内层VLAN的802.1p优先级	**if-match cvlan-8021p** *8021p-value* &<1-8>

匹配规则	命令
MPLS报文EXP优先级（AR1200&AR2200&AR3200&AR3600系列）	**if-match mpls-exp** *exp-value* &<1-8>
目的MAC地址	**if-match destination-mac** *mac-address* [**mac-address-mask** *mac-address-mask*]
源MAC地址	**if-match source-mac** *mac-address* [**mac-address-mask** *mac-address-mask*]
FR报文中的DLCI信息	**if-match dlci** *start-dlci-number* [**to** *end-dlci-number*]
FR报文中的DE标志位	**if-match fr-de**
以太网帧头中协议类型字段	**if-match l2-protocol** { **arp** | **ip** | **mpls** | **rarp** | *protocol-value* }
所有报文	**if-match any**
IP报文的DSCP优先级	**if-match** [**ipv6**] **dscp** *dscp-value* &<1-8> **说明** 如果流策略中配置了匹配DSCP，则SAE220（WSIC）和SAE550（XSIC）单板不支持**redirect ip-nexthop** *ip-address* **post-nat**动作。
IP报文的IP优先级	**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 [ipv6] dscp**和**if-match ip-precedence**。
报文三层协议类型	**if-match protocol** { **ip** | **ipv6** }
指定QoS group索引的IPSec报文	**if-match qos-group** *qos-group-value*
IPv4报文长度	**if-match packet-length** *min-length* [**to** *max-length*]
ATM报文中的PVC信息	**if-match pvc** *vpi-number*/*vci-number*
RTP端口号	**if-match rtp start-port** *start-port-number* **end-port** *end-port-number*
TCP报文SYN Flag	**if-match tcp syn-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** }*
入接口	**if-match inbound-interface** *interface-type interface-number*
出接口	**if-match outbound-interface Cellular** *interface-number:channel*

匹配规则	命令
ACL规则	**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。 ● 当使用ACL作为流分类规则匹配源IP地址时，通过在接口下的**qos pre-nat**配置NAT预分类功能，可以将NAT转换前的私网IP地址信息携带到出接口，即可实现基于私网IP地址的分类，从而对来自不同私网IP地址的报文提供差分服务。
ACL6规则	**if-match ipv6 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。 ● 当使用ACL作为流分类规则匹配源IP地址时，通过在接口下的**qos pre-nat**配置NAT预分类功能，可以将NAT转换前的私网IP地址信息携带到出接口，即可实现基于私网IP地址的分类，从而对来自不同私网IP地址的报文提供差分服务。
应用协议	**if-match application** *application-name* [**user-set** *user-set-name*] [**time-range** *time-name*] **说明** 定义基于应用协议的匹配规则前，必须使能SA功能并加载特征库。
SA协议组	**if-match category** *category-name* [**user-set** *user-set-name*] [**time-range** *time-name*] **说明** ● 定义基于应用协议的匹配规则前，必须使能SA功能并加载特征库。
用户组	**if-match user-set** *user-set-name* [**time-range** *time-range-name*]

d. 执行命令**quit**，退出流分类视图。

2. 配置流行为

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

b. 执行命令**gts cir** { *cir-value* [**cbs** *cbs-value*] | **pct** *pct-value* } [**queue-length** *queue-length*]，配置流量整形动作。

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

d. 执行命令**quit**，退出流行为视图。

e. （可选）执行命令**qos overhead layer** { **link** | **physics** }，配置在流量监管或流量整形时报文长度的计算方式。

缺省情况下，流量监管或流量整形计算报文长度时包括报文的物理层和链路层的补偿信息。

f. 执行命令**quit**，退出系统视图。

3. 配置流策略
   a. 执行命令**system-view**，进入系统视图。
   b. 执行命令**traffic policy** *policy-name*，创建一个流策略并进入流策略视图，或进入已存在的流策略视图。
   c. 执行命令**classifier** *classifier-name* **behavior** *behavior-name*，在流策略中为指定的流分类配置所需流行为，即绑定流分类和流行为。
   d. 执行命令**quit**，退出流策略视图。
   e. 执行命令**quit**，退出系统视图。
4. 应用流策略
   - 在接口下应用流策略
     i. 执行命令**system-view**，进入系统视图。
     ii. 执行命令**interface** *interface-type interface-number* [*.subinterface-number*]，进入接口视图。
     iii. 执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，在接口的入方向或出方向应用流策略。
   - 在安全域间应用流策略

     说明

     仅AR100&AR120&AR150&AR160&AR200系列支持此步骤。

     i. 执行命令**system-view**，进入系统视图。
     ii. 执行命令**firewall interzone** *zone-name1 zone-name2*，创建安全域间并进入安全域间视图。

     缺省情况下，未创建安全域间。

     创建安全域间必须指定两个已存在的安全区域。
     iii. 执行命令**traffic-policy** *policy-name*，在安全域间绑定流策略。

     缺省情况下，安全域间没有绑定流策略。
   - 在BD下应用流策略

     说明

     仅在V200R008C30及之后版本，AR100&AR120&AR150&AR160&AR200&AR1200系列和AR2220E支持此步骤。

     i. 执行命令**system-view**，进入系统视图。
     ii. 执行命令**bridge-domain** *bd-id*，创建广播域BD（Bridge Domain）并进入BD视图。

     缺省情况下，没有创建广播域BD。
     iii. 执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，在BD下应用流策略。

     缺省情况下，BD下没有应用任何流策略。

3.6.5 配置 MQC 实现自适应流量整形

背景信息

若需要对接口出方向的某类流量进行控制时，且下游设备接口速率不确定时，可以配置MQC实现自适应流量整形，当匹配流分类规则的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。基于流的自适应流量整形，可以通过流分类，为不同业务提供更细致的差分服务。

自适应流量整形可以通过在上游设备和下游设备间开启NQA检测，根据NQA检测到的下游设备丢包率动态调整整形参数。

- 当NQA检测到丢包率大于自适应模板配置的丢包率上限，则减小整形速率。
- 当NQA检测到丢包率小于自适应模板配置的丢包率下限，上游发送端接口拥塞，且距离上次增大整形速率的时间间隔超过自适应模板配置的速率增大时间间隔，则增大整形速率。
- 当NQA检测到丢包率小于自适应模板配置的丢包率下限，且上游发送端接口不拥塞，保持当前整形速率。
- 当NQA检测到丢包率在自适应模板配置的丢包率范围内，保持当前整形速率。
- 若NQA检测失败，则整形速率取自适应模板配置的整形速率上限。
- 若自适应模板未绑定NQA测试例，则整形速率取自适应模板配置的整形速率上限。

自适应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，才能使自适应模板中配置的整形参数在该接口下生效。

说明

V200R008C30及以前版本，包含此流行为的流策略只能应用在设备的WAN接口出方向上。

V200R008C50及以后版本，包含此流行为的流策略可以应用在设备的WAN接口和二层VE接口出方向上。

操作步骤

1. 配置自适应模板
   a. 执行命令**system-view**，进入系统视图。
   b. 执行命令**qos adaptation-profile** *adaptation-profile-name*，创建自适应模板，并进入自适应模板视图。
   c. 执行命令**rate-range low-threshold** *low-threshold-value* **high-threshold** *high-threshold-value*，配置自适应模板的整形速率范围。
   d. （可选）执行命令**rate-adjust step** *step*，配置自适应模板的整形速率调整步长。
   e. （可选）执行命令**rate-adjust increase interval** *interval-value*，配置自适应模板中整形速率增大的时间间隔。
   f. （可选）执行命令**rate-adjust loss low-threshold** *low-threshold-percentage* **high-threshold** *high-threshold-percentage*，配置自适应模板的丢包率范围。
   g. 执行命令**track nqa** *admin-name test-name*，为自适应模板绑定NQA测试例。

      说明

      配置NQA测试例时，需保证NQA探测报文的优先级别，确保报文能够进入高优先级队列，不会在链路流量较大时被丢弃。

   h. 执行命令**quit**，退出自适应模板视图。
   i. 执行命令**quit**，退出系统视图。
2. 配置流分类
   a. 执行命令**system-view**，进入系统视图。

b. 执行命令**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]，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”，指定该逻辑关系后：

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

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

缺省情况下，流分类中各规则之间的关系为“逻辑或”。

c. 请根据实际情况配置流分类中的匹配规则。

匹配规则	命令
外层VLAN ID	**if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*]
QinQ报文内层VLAN ID	**if-match cvlan-id** *start-vlan-id* [**to** *end-vlan-id*]
VLAN报文802.1p优先级	**if-match 8021p** *8021p-value* &<1-8>
QinQ报文内层VLAN的802.1p优先级	**if-match cvlan-8021p** *8021p-value* &<1-8>
MPLS报文EXP优先级（AR1200&AR2200&AR3200&AR3600系列）	**if-match mpls-exp** *exp-value* &<1-8>
目的MAC地址	**if-match destination-mac** *mac-address* [**mac-address-mask** *mac-address-mask*]
源MAC地址	**if-match source-mac** *mac-address* [**mac-address-mask** *mac-address-mask*]
FR报文中的DLCI信息	**if-match dlci** *start-dlci-number* [**to** *end-dlci-number*]
FR报文中的DE标志位	**if-match fr-de**
以太网帧头中协议类型字段	**if-match l2-protocol** { **arp** | **ip** | **mpls** | **rarp** | *protocol-value* }
所有报文	**if-match any**
IP报文的DSCP优先级	**if-match** [**ipv6**] **dscp** *dscp-value* &<1-8> **说明** 如果流策略中配置了匹配DSCP，则SAE220（WSIC）和SAE550（XSIC）单板不支持**redirect ip-nexthop** *ip-address* **post-nat**动作。

匹配规则	命令
IP报文的IP优先级	**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 [ipv6] dscp**和**if-match ip-precedence**。
报文三层协议类型	**if-match protocol** { **ip** | **ipv6** }
指定QoS group索引的IPSec报文	**if-match qos-group** *qos-group-value*
IPv4报文长度	**if-match packet-length** *min-length* [**to** *max-length*]
ATM报文中的PVC信息	**if-match pvc** *vpi-number/vci-number*
RTP端口号	**if-match rtp start-port** *start-port-number* **end-port** *end-port-number*
TCP报文SYN Flag	**if-match tcp syn-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** }*
入接口	**if-match inbound-interface** *interface-type interface-number*
出接口	**if-match outbound-interface Cellular** *interface-number:channel*
ACL规则	**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。 ● 当使用ACL作为流分类规则匹配源IP地址时，通过在接口下的**qos pre-nat**配置NAT预分类功能，可以将NAT转换前的私网IP地址信息携带到出接口，即可实现基于私网IP地址的分类，从而对来自不同私网IP地址的报文提供差分服务。
ACL6规则	**if-match ipv6 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。 ● 当使用ACL作为流分类规则匹配源IP地址时，通过在接口下的**qos pre-nat**配置NAT预分类功能，可以将NAT转换前的私网IP地址信息携带到出接口，即可实现基于私网IP地址的分类，从而对来自不同私网IP地址的报文提供差分服务。
应用协议	**if-match application** *application-name* [**user-set** *user-set-name*] [**time-range** *time-name*] **说明** 定义基于应用协议的匹配规则前，必须使能SA功能并加载特征库。

匹配规则	命令
SA协议组	**if-match category** *category-name* [**user-set** *user-set-name*] [**time-range** *time-name*] **说明** ● 定义基于应用协议的匹配规则前，必须使能SA功能并加载特征库。
用户组	**if-match user-set** *user-set-name* [**time-range** *time-range-name*]

d. 执行命令**quit**，退出流分类视图。

3. 配置流行为
   a. 执行命令**traffic behavior** *behavior-name*，创建一个流行为，进入流行为视图。
   b. 执行命令**gts adaptation-profile** *adaptation-profile-name*，在流行为中绑定已创建的自适应模板。

      说明
      自适应模板必须已经创建并配置。
   c. （可选）执行命令**statistic enable**，使能流量统计功能。
   d. 执行命令**quit**，退出流行为视图。
   e. （可选）执行命令**qos overhead layer** { **link** | **physics** }，配置在流量监管或流量整形时报文长度的计算方式。

      缺省情况下，流量监管或流量整形计算报文长度时包括报文的物理层和链路层的补偿信息。
   f. 执行命令**quit**，退出系统视图。
4. 配置流策略
   a. 执行命令**system-view**，进入系统视图。
   b. 执行命令**traffic policy** *policy-name*，创建一个流策略并进入流策略视图，或进入已存在的流策略视图。
   c. 执行命令**classifier** *classifier-name* **behavior** *behavior-name*，在流策略中为指定的流分类配置所需流行为，即绑定流分类和流行为。
   d. 执行命令**quit**，退出流策略视图。
   e. 执行命令**quit**，退出系统视图。
5. 应用流策略
   - 在接口下应用流策略
     i. 执行命令**system-view**，进入系统视图。
     ii. 执行命令**interface** *interface-type interface-number* [*.subinterface-number*]，进入接口视图。
     iii. 执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，在接口的入方向或出方向应用流策略。
   - 在安全域间应用流策略

     说明
     仅AR100&AR120&AR150&AR160&AR200系列支持此步骤。

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**firewall interzone** *zone-name1 zone-name2*，创建安全域间并进入安全域间视图。

缺省情况下，未创建安全域间。

创建安全域间必须指定两个已存在的安全区域。

iii. 执行命令**traffic-policy** *policy-name*，在安全域间绑定流策略。

缺省情况下，安全域间没有绑定流策略。

- 在BD下应用流策略

说明

仅在V200R008C30及之后版本，AR100&AR120&AR150&AR160&AR200&AR1200系列和AR2220E支持此步骤。

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**bridge-domain** *bd-id*，创建广播域BD（Bridge Domain）并进入BD视图。

缺省情况下，没有创建广播域BD。

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

缺省情况下，BD下没有应用任何流策略。

3.6.6 检查配置结果

操作步骤

- 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 applied-record** [*policy-name*]，查看指定流量整形策略的应用记录信息。
- 检查自适应模板的配置结果
  - 执行命令**display qos adaptation-profile** [*adaptation-profile-name*]，查看自适应模板的配置信息。
  - 执行命令**display qos adaptation-profile** *adaptation-profile-name* [**interface** *interface-type interface-number*] **applied-record**，查看自适应模板的应用记录。

----结束

3.7 配置物理接口限速

WAN侧物理接口支持接口限速功能，通过配置接口发送报文速率占接口带宽的百分比，实现对接口发送报文速率的限制。

前置任务

在配置物理接口限速之前，需要完成以下任务：

- 配置相关接口的链路层属性，保证接口的正常工作

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 （可选）执行命令**qos overhead layer** { **link** | **physics** }，配置在流量监管或流量整形时报文长度的计算方式。

缺省情况下，流量监管或流量整形计算报文长度时包括报文的物理层和链路层的补偿信息。

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

步骤4 执行命令**qos lr pct** *pct-value* [**cbs** *cbs-value*]，配置接口发送报文速率占接口带宽的百分比。

缺省情况下，接口发送报文速率占接口带宽的百分比为100。

说明

接口上需要配置队列，接口限速才会生效。

----结束

检查配置结果

- 在配置了限速功能的接口上，进入接口视图，执行命令**display this**，查看接口限速功能的配置信息。

3.8 维护流量监管和流量整形

流量监管和流量整形的维护，包括查看流量统计信息、清除流量统计数据。

3.8.1 查看流量统计信息

背景信息

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

- 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* [**son-class** *son-class-name*]]]或**display traffic policy statistics interface virtual-template** *vt-number* **virtual-access** *va-number* { **inbound** | **outbound** } [**verbose** { **classifier-base** | **rule-base** } [**class** *classifier-name* [**son-class** *son-class-name*]]]，查看基于流的流量统计信息。

- 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* [**queue** *queue-index*]，查看基于队列的流量统计信息。

----结束

3.8.2 清除流量统计信息

背景信息

注意

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

操作步骤

- 执行命令**reset traffic policy statistics interface** *interface-type interface-number* [**pvc** *vpi-number/vci-number* | **dlci** *dlic-number*] { **inbound** | **outbound** }或**reset traffic policy statistics interface virtual-template** *vt-number* **virtual-access** *va-number* { **inbound** | **outbound** }，清除指定接口下应用的流策略的统计信息。
- 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* [**queue** *queue-index*]，清除接口上基于队列的流量统计信息。

----结束

3.9 配置举例

通过示例介绍配置流量监管和流量整形。配置示例中包括组网需求、配置注意事项、配置思路等。

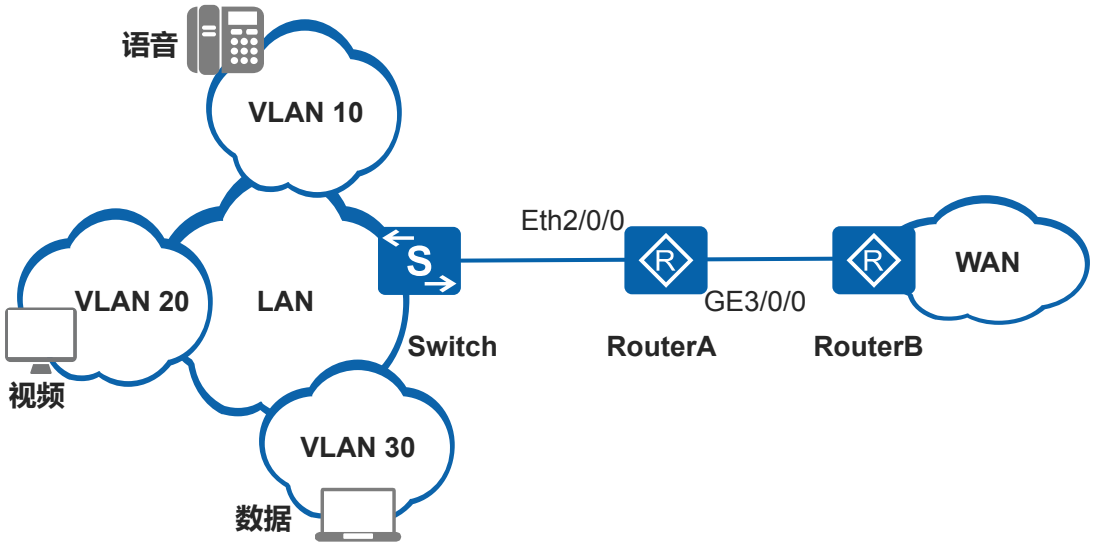
3.9.1 配置流量监管示例

组网需求

如图3-8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Eth2/0/0上，通过RouterA的GE3/0/0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Eth2/0/0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 3-8 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。

操作步骤

步骤1 创建VLAN并配置各接口

在RouterA上创建VLAN10、VLAN20和VLAN30。

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

配置接口Eth2/0/0为Trunk类型端口，并允许VLAN10、VLAN20和VLAN30的报文通过。

```
[RouterA] interface ethernet 2/0/0
[RouterA-Ethernet2/0/0] port link-type trunk
[RouterA-Ethernet2/0/0] port trunk allow-pass vlan 10 20 30
[RouterA-Ethernet2/0/0] quit
```

说明

请配置Switch与RouterA对接的接口为Trunk类型接口，并允许VLAN10、VLAN20和VLAN30的报文通过。

创建VLANIF10、VLANIF20和VLANIF30，并为VLANIF10配置IP地址192.168.1.1/24，并为VLANIF20配置IP地址192.168.2.1/24，为VLANIF30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GE3/0/0的IP地址为192.168.4.1/24。

```
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] ip address 192.168.4.1 24
[RouterA-GigabitEthernet3/0/0] quit
```

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。

```
[RouterA] traffic behavior b1
[RouterA-behavior-b1] car cir 256
[RouterA-behavior-b1] statistic enable
[RouterA-behavior-b1] quit
[RouterA] traffic behavior b2
[RouterA-behavior-b2] car cir 4000
[RouterA-behavior-b2] statistic enable
[RouterA-behavior-b2] quit
[RouterA] traffic behavior b3
[RouterA-behavior-b3] car cir 2000
[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Eth2/0/0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 2/0/0
[RouterA-Ethernet2/0/0] traffic-policy p1 inbound
```

步骤5 配置基于接口的流量监管

在RouterA的接口Eth2/0/0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-Ethernet2/0/0] qos car inbound cir 10000
[RouterA-Ethernet2/0/0] 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 2/0/0 inbound

 Interface: Ethernet2/0/0
 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 Ethernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 10 20 30
 qos car inbound cir 10000
 traffic-policy p1 inbound
```

```
#
interface GigabitEthernet3/0/0
 ip address 192.168.4.1 255.255.255.0
#
return
```

相关资料

视频：配置基于接口的限速

3.9.2 配置流量整形示例

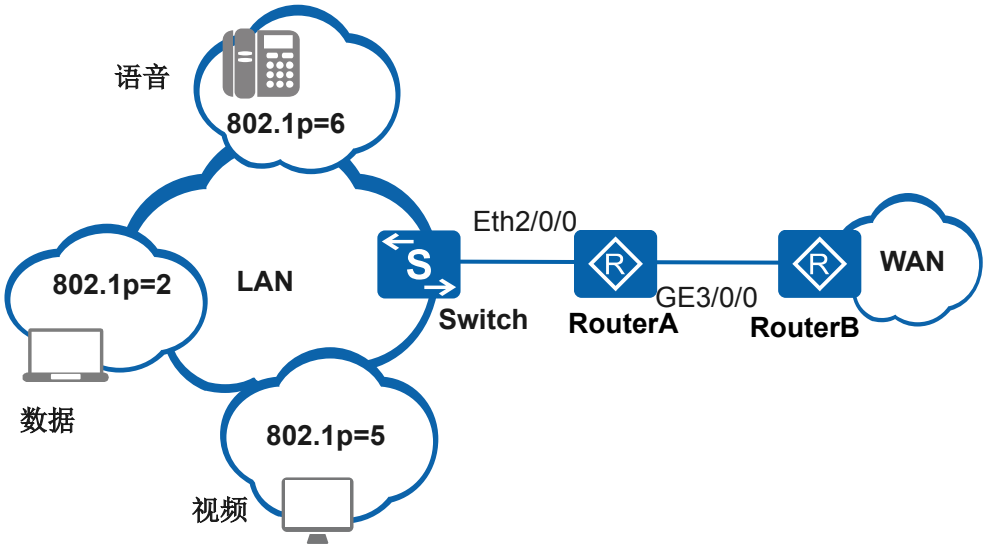
组网需求

如图3-9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Eth2/0/0上，并通过RouterA的GE3/0/0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GE3/0/0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 3-9 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。

操作步骤

步骤1 创建VLAN并配置各接口

在RouterA上创建VLAN 10。

```
<Router> system-view
[Router] sysname RouterA
[RouterA] vlan 10
[RouterA-vlan10] quit
```

配置接口Eth2/0/0为Trunk类型端口，并将Eth2/0/0加入VLAN10。

```
[RouterA] interface ethernet 2/0/0
[RouterA-Ethernet2/0/0] port link-type trunk
[RouterA-Ethernet2/0/0] port trunk allow-pass vlan 10
[RouterA-Ethernet2/0/0] 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GE3/0/0的IP地址为192.168.4.1/24。

```
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] ip address 192.168.4.1 24
[RouterA-GigabitEthernet3/0/0] 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Eth2/0/0接口信任报文的802.1p优先级。

```
[RouterA] interface ethernet 2/0/0
[RouterA-Ethernet2/0/0] trust 8021p
[RouterA-Ethernet2/0/0] 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 gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] qos gts cir 8000
[RouterA-GigabitEthernet3/0/0] 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GE3/0/0上应用队列模板qp1。

```
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] qos queue-profile qp1
```

步骤5 验证配置结果

查看RouterA接口的配置信息。

```
[RouterA-GigabitEthernet3/0/0] display this
#
interface GigabitEthernet3/0/0
 ip address 192.168.4.1 255.255.255.0
 qos queue-profile qp1
 qos gts cir 8000
#
return
```

查看在接口上应用的队列模板信息。

```
[RouterA-GigabitEthernet3/0/0] 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 batch 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 Ethernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 10
 trust 8021p
#
interface GigabitEthernet3/0/0
  ip address 192.168.4.1 255.255.255.0
 qos queue-profile qp1
 qos gts cir 8000
#
return
```

3.9.3 配置自适应流量整形示例

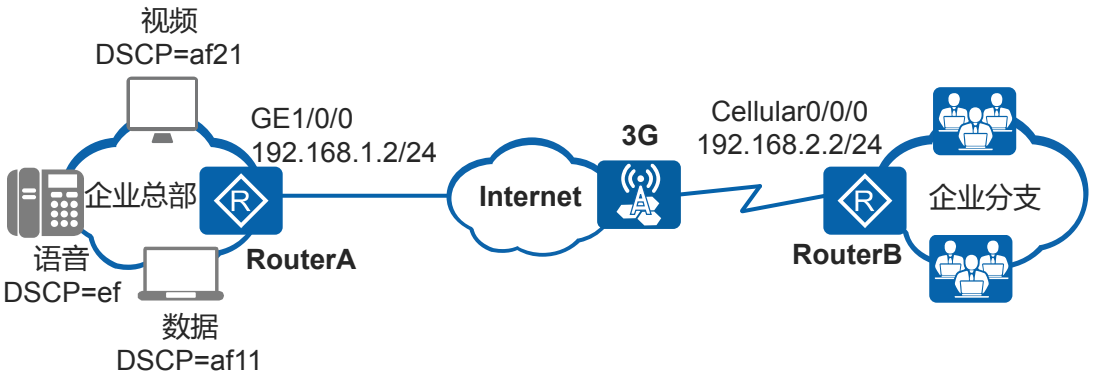
组网需求

如图3-10所示，企业总部的业务通过RouterA的接口GE1/0/0连接到Internet，并通过3G网络连接到分支RouterB，从而实现总部和分支的通信。

由于分支使用3G网络接入，链路带宽不稳定，企业希望总部发送报文的速率能够随3G链路带宽变化动态调整，以减少3G网络中的带宽抖动。

同时，企业总部发往分支的报文中，数据、视频和语音报文的DSCP优先级分别为af11、af21和ef，企业希望语音报文能够保证优先发送，视频、数据报文能够保证带宽。

图 3-10 配置自适应流量整形的组网图



配置思路

采用基于接口的自适应流量整形来实现总部发送报文速率的动态调整，采用基于流的拥塞管理来实现语音、视频和数据报文的不同处理，具体配置思路如下：

1. 在RouterA和RouterB上配置Jitter类型的NQA测试例，实现对总部与分支间链路状态的检测。
2. 在RouterA上配置自适应整形模板并应用到接口GE1/0/0上，当NQA测试例连续三次检测到链路中报文丢包率超过30%时，降低接口GE1/0/0发送报文的速率，实现总部发送报文速率的动态调整。
3. 在RouterA上配置流分类，实现对数据、视频、语音报文的区分。
4. 在RouterA配置流行为，针对数据、视频、语音报文，指定不同的拥塞管理动作。
5. 在RouterA上配置流策略，将流分类和对应流行为关联起来并应用到接口GE1/0/0上，实现对数据、视频和语音报文的不同处理。

操作步骤

步骤1 配置NQA测试例

配置NQA服务器UDP使用的IP地址和端口号。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] nqa-server udpecho 192.168.2.2 9000
```

使能NQA客户端，配置Jitter类型的NQA测试例。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] nqa test-instance admin jitter1
[RouterA-nqa-admin-jitter1] test-type jitter
[RouterA-nqa-admin-jitter1] destination-address ipv4 192.168.2.2
[RouterA-nqa-admin-jitter1] destination-port 9000
[RouterA-nqa-admin-jitter1] start now
[RouterA-nqa-admin-jitter1] quit
```

步骤2 在RouterA上配置自适应整形模板

```
[RouterA] qos adaptation-profile gts1
[RouterA-qos-adaptation-profile-gts1] rate-range low-threshold 128 high-threshold 512
[RouterA-qos-adaptation-profile-gts1] rate-adjust step 32
[RouterA-qos-adaptation-profile-gts1] rate-adjust loss low-threshold 20 high-threshold 30
[RouterA-qos-adaptation-profile-gts1] track nqa admin jitter1
[RouterA-qos-adaptation-profile-gts1] quit
```

步骤3 在RouterA的接口GE1/0/0上应用自适应整形模板

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] qos gts adaptation-profile gts1
[RouterA-GigabitEthernet1/0/0] quit
```

步骤4 在RouterA上配置流分类，区分出数据、视频和语音业务

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

步骤5 在RouterA上配置流行为，配置匹配分类规则的报文进入指定队列并为其分配带宽

```
[RouterA] traffic behavior data
[RouterA-behavior-data] queue af bandwidth pct 30
[RouterA-behavior-data] quit
[RouterA] traffic behavior video
[RouterA-behavior-video] queue af bandwidth pct 60
[RouterA-behavior-video] quit
[RouterA] traffic behavior voice
[RouterA-behavior-voice] queue llq bandwidth pct 5
[RouterA-behavior-voice] quit
```

步骤6 在RouterA上创建流策略，将流分类和对应流行为关联起来

```
[RouterA] traffic policy p1
[RouterA-trafficpolicy-p1] classifier voice  behavior voice
[RouterA-trafficpolicy-p1] classifier video  behavior video
[RouterA-trafficpolicy-p1] classifier data  behavior  data
[RouterA-trafficpolicy-p1] quit
```

步骤7 在RouterA上将流策略应用到接口GE1/0/0上

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 192.168.1.2 24
[RouterA-GigabitEthernet1/0/0] traffic-policy p1 outbound
[RouterA-GigabitEthernet1/0/0] quit
```

步骤8 验证配置结果

查看自适应模板gts1在RouterA接口GE1/0/0的应用记录。

```
[RouterA] display qos adaptation-profile gts1 interface gigabitethernet 1/0/0 applied-record
Interface: GigabitEthernet1/0/0
------------------------------------------------------------------
 QoS gts adaptation-profile: gts1
------------------------------------------------------------------
NQA admin Name: admin
NQA test Name: jitter1
Current Rate: 256(Kbps)
Last packet loss: 25(%)
The latest traffic shaping rate fails to be updated because the packet loss ratio is within the
allowed range.
```

----结束

配置文件

- RouterA的配置文件

```
#
 sysname RouterA
#
qos adaptation-profile gts1
 rate-range low-threshold 128 high-threshold 512
 track nqa admin jitter1
 rate-adjust loss low-threshold 20 high-threshold 30
 rate-adjust step 32
#
traffic classifier video operator or
 if-match dscp af21
traffic classifier data operator or
 if-match dscp af11
traffic classifier voice operator or
 if-match dscp ef
#
traffic behavior video
 queue af bandwidth pct 60
traffic behavior data
 queue af bandwidth pct 30
traffic behavior voice
 queue llq bandwidth pct 5
#
traffic policy p1
 classifier voice behavior voice
 classifier video behavior video
 classifier data behavior data
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.2 255.255.255.0
 qos gts adaptation-profile gts1
 traffic-policy p1 outbound
#
nqa test-instance admin jitter1
 test-type jitter
 destination-address ipv4 192.168.2.2
 destination-port 9000
#
return
```

- RouterB的配置文件

```
#
 sysname RouterB
#
nqa-server udpecho 192.168.2.2 9000
#
return
```

3.10 FAQ

介绍配置流量监管和流量整形的FAQ。

3.10.1 设备是否支持基于每个 IP 地址进行限速

V200R002C00以后版本可以通过**qos car**命令基于每个IP地址进行限速。

3.10.2 设备如何保证不同流量的带宽

在设备上配置流分类区分不同的流量，然后在流行为中通过**queue ef**或者**queue af**命令对不同流量进行带宽保证，最后将流策略绑定在接口上。

3.10.3 在 WAN 侧口配置 IP CAR 为何不生效

由于在WAN侧口上配置了NAT，设备无法对私网地址进行区分，因此IP CAR不生效。

V200R002C00及以后的版本，若要在WAN侧口配置IP CAR，可以在设备上新建VLANIF接口，在VLANIF接口上配置IP CAR。

- 若限制用户下载速率，请配置指定目的IP地址和出方向的IP CAR。
- 若限制用户上传速率，请配置指定源IP地址和入方向的IP CAR。

3.10.4 二层口上能否配置基于 IP 进行限速的功能

不能。请在设备上新建VLANIF接口，在VLANIF接口上配置基于IP进行限速的功能。

3.10.5 出向流量监管和端口整形 GTS 限速的区别

出向流量监管和端口整形都是对端口出向的流量进行限速，两者功能比较相似，不同点是：

- 流量监管进行报文限速时，直接丢弃不符合速率要求的报文；流量整形则会将不符合速率要求的报文先进行缓存，再均匀的向外发送这些被缓存的报文。
- 流量整形可能会增加延迟，而流量监管几乎不引入额外的延迟。

3.10.6 能否在接口出方向同时配置 qos gts 和 qos car

由于**qos car**会影响**qos gts**的效果，建议不要同时配置。

3.10.7 自适应模板为什么可以配置整形速率增大的时间间隔，不可配置整形速率减小的时间间隔？

当NQA检测到丢包率大于自适应模板配置的丢包率上限，则立即减小整形速率。这样实现是为了保证整形速率快速调整至网络适应的速率，避免业务数据进一步丢失。

3.10.8 自适应模板是否允许不绑定 NQA 测试例？

允许，若自适应模板未绑定NQA测试例，则整形速率取自适应模板配置的整形速率上限。

3.10.9 自适应模板默认按照整形速率范围的上限还是下限生效？

默认初始按照速率上限生效，然后根据NQA检测到的下游设备丢包率动态调整整形参数。

3.11 参考信息

介绍QoS特性的相关参考资料。

文档	描述	备注
RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	-
RFC 2475	An Architecture for Differentiated Services	-
RFC 2597	Assured Forwarding PHB Group	-
RFC 2598	An Expedited Forwarding PHB	-
RFC 2697	A Single Rate Three Color Marker	-
RFC 2698	A Two Rate Three Color Marker	-

4 拥塞管理和拥塞避免配置

关于本章

通过配置拥塞管理和拥塞避免，当网络中发生拥塞时，设备按照一定的调度策略决定报文的转发次序，使关键业务得到优先处理，或者主动丢弃报文，通过调整网络流量来解除网络过载。

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

4.2 原理描述
介绍了拥塞管理和拥塞避免的原理和实现方式等。

4.3 应用场景

4.4 缺省配置
拥塞管理和拥塞避免缺省配置介绍了拥塞管理和拥塞避免常用参数的缺省配置。

4.5 配置拥塞管理
配置拥塞管理后，当网络中发生拥塞时，设备将按照配置的调度策略决定报文转发时的处理次序，确保高优先级业务优先发送。

4.6 配置拥塞避免
配置拥塞避免后，设备将根据配置的丢弃模板主动丢弃超出流量范围的报文，以调整网络流量，解除网络过载。

4.7 配置举例
通过示例介绍如何应用拥塞管理和拥塞避免。配置示例中包括组网需求、配置注意事项、配置思路等。

4.8 FAQ
介绍配置拥塞管理和拥塞避免的FAQ。

4.9 参考信息

4.1 拥塞避免和拥塞管理概述

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

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

拥塞避免和拥塞管理就是解决网络拥塞的两种流控方式。

拥塞避免

拥塞避免是指通过监视网络资源（如队列或内存缓冲区）的使用情况，在拥塞发生或有加剧趋势时主动丢弃报文，通过调整网络的流量来解除网络过载的一种流量控制机制。

设备支持以下拥塞避免功能：

- 尾部丢弃

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

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

- WRED

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

  WRED技术为每个队列的长度都设定了阈值上下限，并规定：

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

拥塞管理

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

设备支持以下拥塞管理功能：

- PQ调度

  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得不到调度机会。

- WRR调度

  WRR（Weighted Round Robin）调度即加权轮询调度。WRR在队列之间进行轮流调度，保证每个队列都得到一定的服务时间。

  以端口有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可能长期得不到调度，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。

    设备除了提供普通的EF队列，还支持一种特殊的EF队列—LLQ队列，时延更低。这为对时延敏感的应用（如VoIP业务）提供了良好的服务质量保证。

    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。

  说明

  分片报文在经过队列调度后，可能会随机丢弃部分报文，从而导致分片报文重组失败。

4.2 原理描述

介绍了拥塞管理和拥塞避免的原理和实现方式等。

4.2.1 拥塞避免

拥塞避免（Congestion Avoidance）是指通过监视网络资源（如队列或内存缓冲区）的使用情况，在拥塞发生或有加剧的趋势时主动丢弃报文，通过调整网络的流量来解除网络过载的一种流控机制。

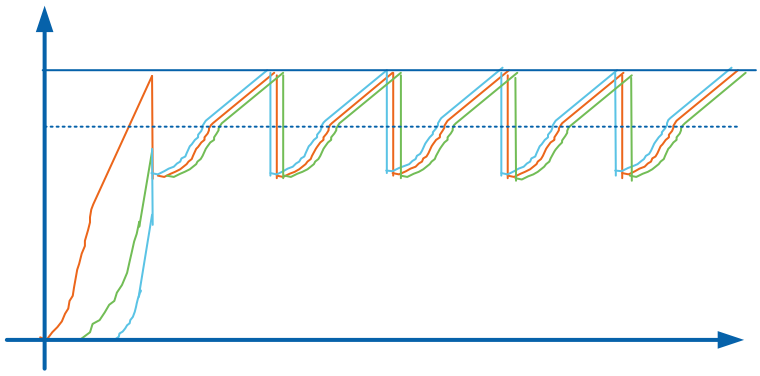
拥塞避免常用的两种丢弃报文方式为：尾部丢包策略和WRED。

- 传统的尾部丢包策略

  传统的丢包策略采用尾部丢弃（Tail-Drop）的方法。当队列的长度达到最大值后，所有新入队列的报文（缓存在队列尾部）都将被丢弃。

  这种丢弃策略会引发TCP全局同步现象，导致TCP连接始终无法建立。所谓TCP全局同步现象如图，三种颜色表示三条TCP连接，当同时丢弃多个TCP连接的报文时，将造成多个TCP连接同时进入拥塞避免和慢启动状态而导致流量降低，之后又会在某个时间同时出现流量高峰，如此反复，使网络流量忽大忽小。

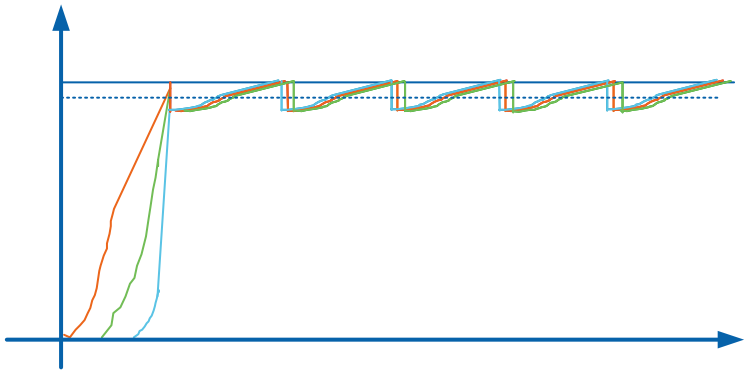
  图 4-1 尾部丢包示意图

- WRED

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

  图 4-2 RED 算法示意图

  基于RED技术，设备实现了WRED（Weighted Random Early Detection）。流队列支持基于DSCP或IP优先级进行WRED丢弃。每一种优先级都可以独立设置报文丢包的上下门限及丢包率，报文到达下限时，开始丢包，随着门限的增高，丢包率不断增加，最高丢包率不超过设置的丢包率，直至到达高门限，报文全部丢弃，这样按照一定的丢弃概率主动丢弃队列中的报文，从而一定的程度上避免拥塞问题。

  说明

  V200R008C30及以前版本，LAN侧接口板不支持WRED。V200R008C50及以后版本，二层VE接口支持WRED。

4.2.2 拥塞管理

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

根据排队和调度策略的不同，WAN接口和二层VE接口上的拥塞管理技术分为PQ、WFQ和PQ+WFQ，设备其余LAN接口上的拥塞管理技术分为PQ、DRR、PQ+DRR、WRR、PQ+WRR。

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

- PQ调度

  PQ调度，针对于关键业务类型应用设计，PQ调度算法维护一个优先级递减的队列系列并且只有当更高优先级的所有队列为空时才服务低优先级的队列。这样，将关键业务的分组放入较高优先级的队列，将非关键业务（如E-Mail）的分组放入较低优先级的队列，可以保证关键业务的分组被优先传送，非关键业务的分组在处理关键业务数据的空闲间隙被传送。

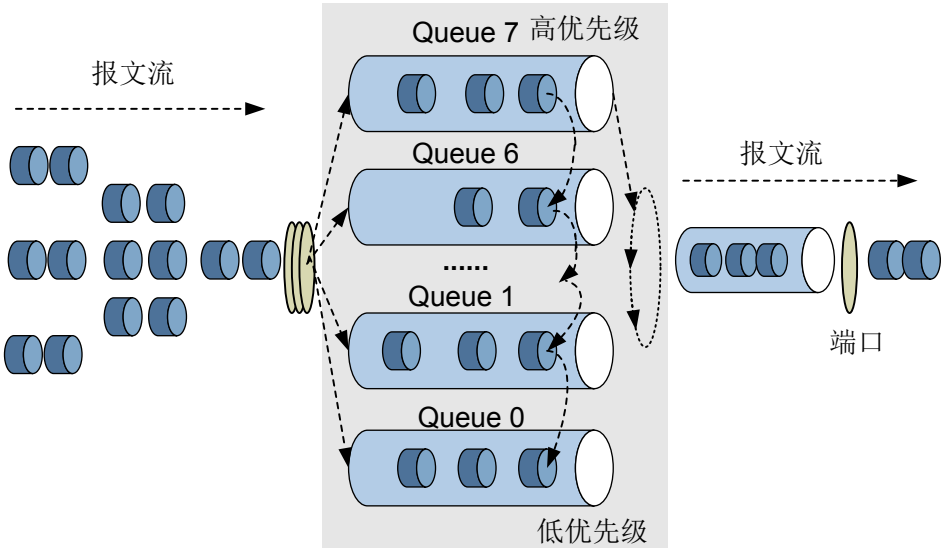
  如图4-3所示，Queue7比Queue6具有更高的优先权，Queue6比Queue5具有更高的优先权，依次类推。只要链路能够传输分组，Queue7尽可能快地被服务。只有当Queue7为空，调度器才考虑Queue6。当Queue6有分组等待传输且Queue7为空时，Queue6以链路速率接受类似地服务。当Queue7和Queue6为空时，Queue5以链路速率接收服务，以此类推。

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

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

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

图 4-3 PQ 调度示意图

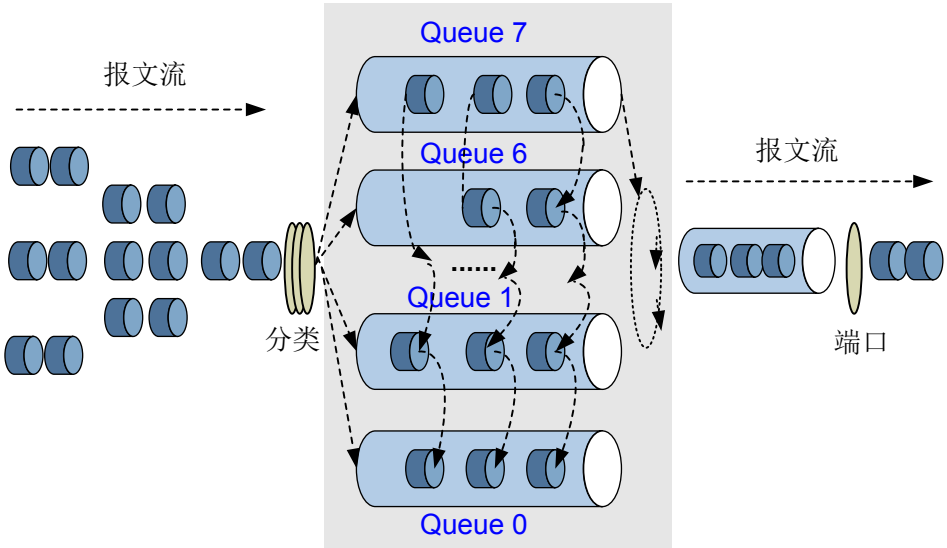


- WRR调度

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

  WRR队列示意图如图4-4所示。

图 4-4 WRR 调度示意图



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

表 4-1 WRR 调度的结果

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

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

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

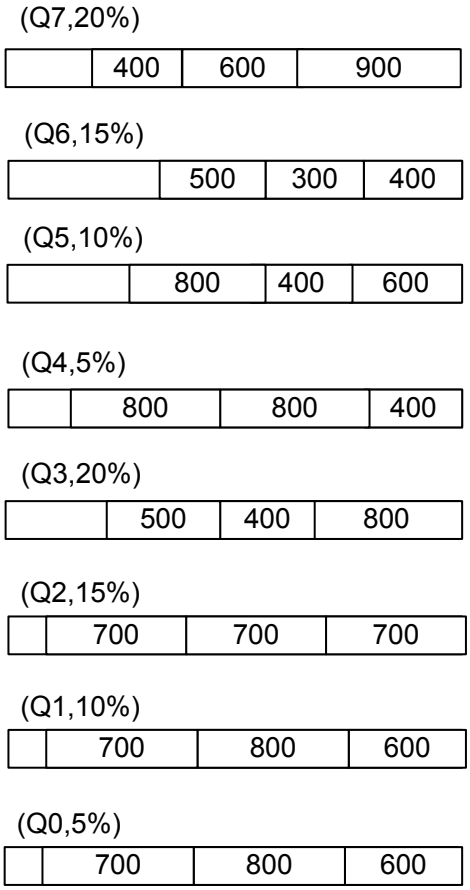
WRR调度避免了采用PQ调度时低优先级队列中的报文可能长时间得不到服务的缺点。WRR队列还有一个优点是，虽然多个队列的调度是轮询进行的，但对每个队列不是固定地分配服务时间片——如果某个队列为空，那么马上换到下一个队列调度，这样带宽资源可以得到充分的利用。但WRR调度无法使低延时需求业务得到及时调度。

- DRR调度

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

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

图 4-5 队列权重示意图



如图4-5所示，假设用户配置各队列权重为40、30、20、10、40、30、20、10（依次对应Q7、Q6、Q5、Q4、Q3、Q2、Q1、Q0），调度时，队列Q7、Q6、Q5、Q4、Q3、Q2、Q1、Q0依次能够获取20%、15%、10%、5%、20%、15%、10%、5%的带宽。下面以Q7、Q6为例，简要描述DRR队列调度的实现过程（假设Q7队列获取400byte/s的带宽，Q6队列获取300byte/s的带宽）。

- 第1轮调度

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

- 第2轮调度

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

- 第3轮调度

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

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

但DRR调度仍然没有解决WRR调度中低延时需求业务得不到及时调度的问题。

- WFQ调度

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

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

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

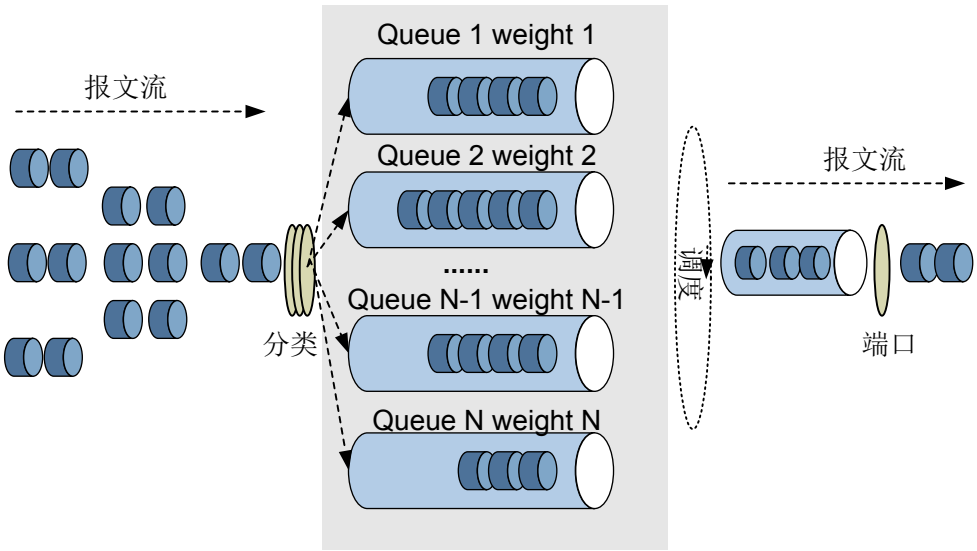
  WFQ调度在报文入队列之前，先对流量进行分类，有两种分类方式：

  - 按流的“会话”信息分类：

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

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

图 4-6 WFQ 调度示意图

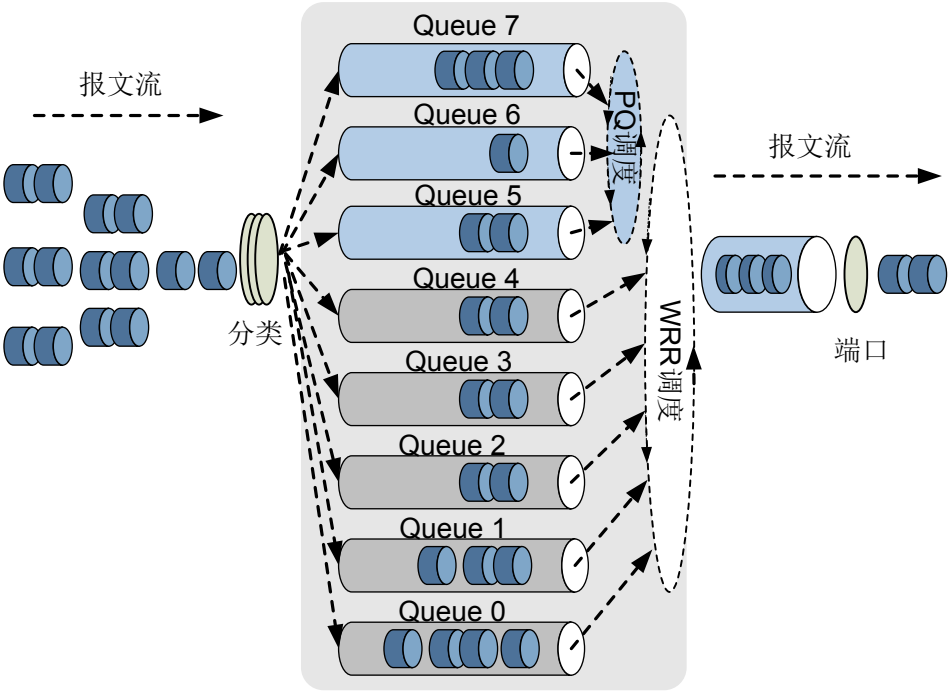


- PQ+WRR调度

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

在设备上，用户可以配置队列的WRR参数，根据配置将接口上的8个队列分为两组，一组（例如Queue7、Queue6、Queue5）采用PQ调度，另一组（例如Queue4、Queue3、Queue2、Queue1和Queue0队列）采用WRR调度。设备上只有LAN侧接口支持PQ+WRR调度。PQ+WRR调度示意图如图4-7所示。

图 4-7 PQ+WRR 混合调度示意图



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

- PQ+DRR调度

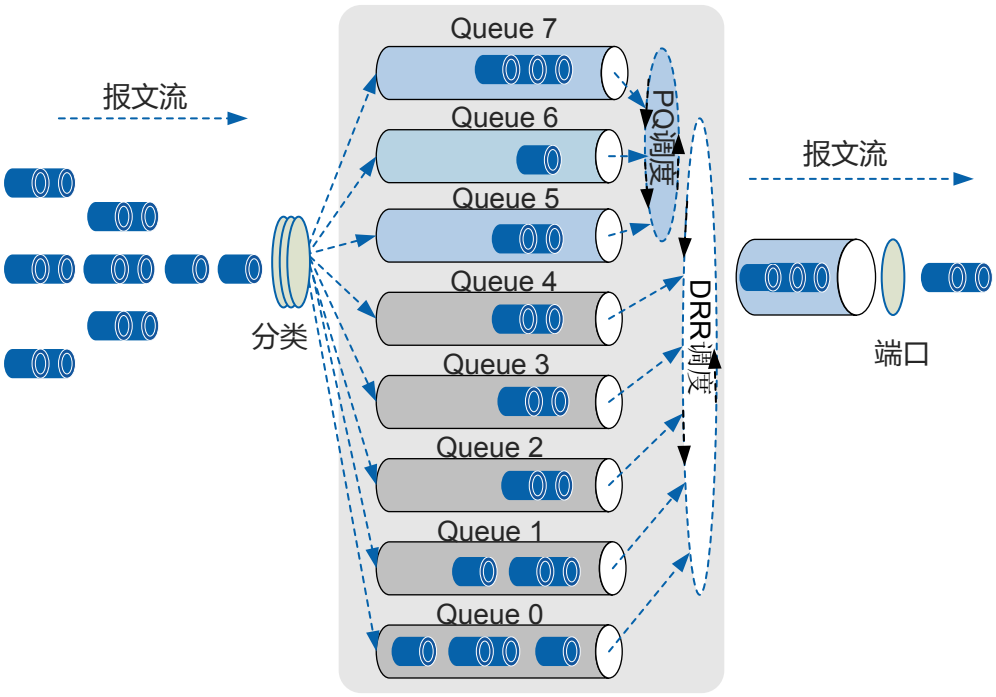
  说明

  设备的LAN侧接口支持PQ+DRR调度。

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

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

图 4-8 PQ+DRR 调度示意图



如图4-8所示，在调度时，设备首先按照PQ方式优先调度Queue7、Queue6和Queue5队列中的报文流，只有这些队列中的报文流全部调度完毕后，才开始以DRR方式调度Queue4、Queue3、Queue2、Queue1和Queue0队列中的报文流。其中，Queue4、Queue3、Queue2、Queue1和Queue0队列包含自己的权值。

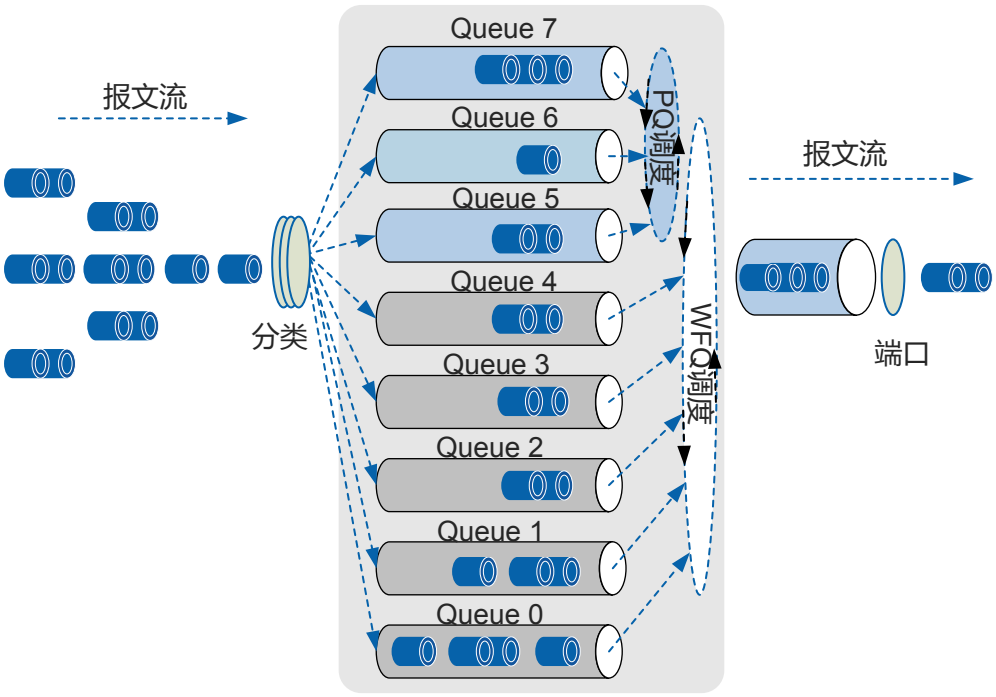
重要的协议报文以及有低延时需求的业务报文应放入需要进行PQ调度的队列中，得到优先调度的机会，其他报文放入以DRR方式调度的各队列中。

- PQ+WFQ调度

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

  设备接口上的8个队列被分为两组，用户可以指定其中的某几组队列进行PQ调度，其他队列进行WFQ调度。V200R008C30及以前版本，只有WAN侧接口支持PQ+WFQ调度。V200R008C50及以后版本，WAN侧接口和二层VE接口支持PQ+WFQ调度。

图 4-9 PQ+WFQ 调度示意图



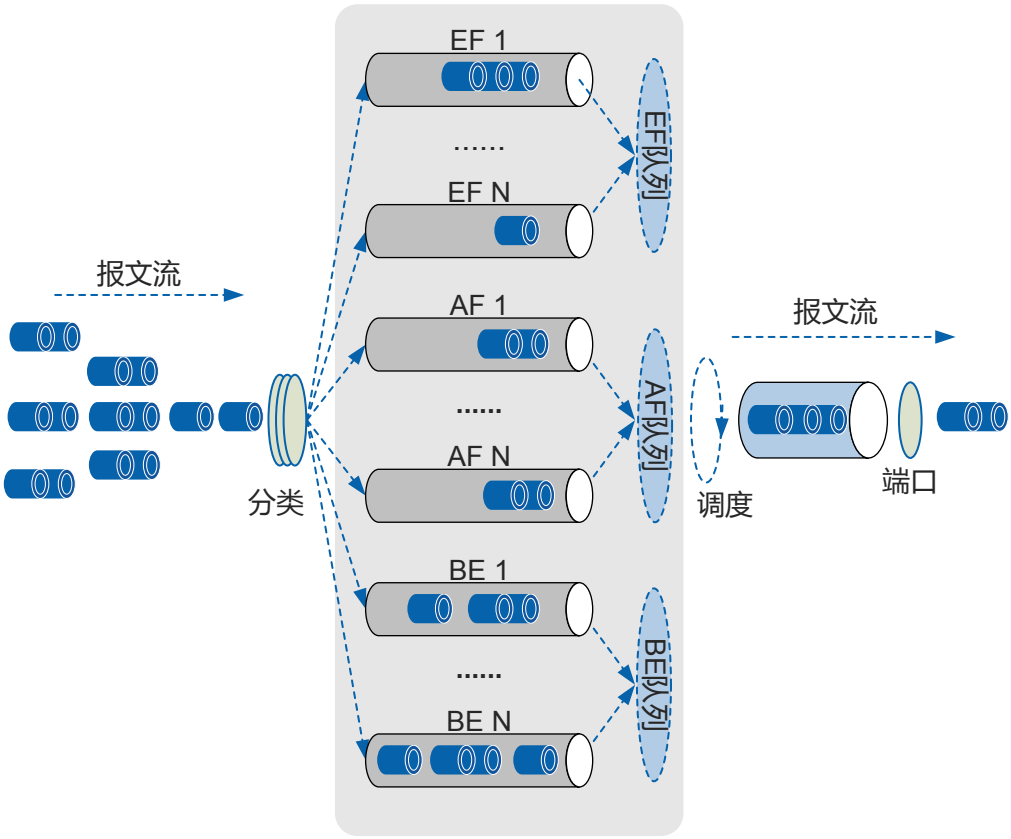
如图4-9所示，在调度时，设备首先按照PQ方式优先调度Queue7、Queue6和Queue5队列中的报文流，只有这些队列中的报文流全部调度完毕后，才开始以WFQ方式调度Queue4、Queue3、Queue2、Queue1和Queue0队列中的报文流。其中，Queue4、Queue3、Queue2、Queue1和Queue0队列包含自己的权值。

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

- CBQ调度

  CBQ（Class-based Queueing）基于类的加权公平队列是对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。

图 4-10 CBQ 调度示意图



如图4-10所示CBQ提供三类队列：

- EF队列：满足低时延业务
- AF队列：满足需要带宽保证的关键数据业务
- BE队列：满足不需要严格QoS保证的尽力发送业务
- EF队列

  EF队列是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，会优先得到调度，以保证其获得低时延。当接口发生拥塞时，EF队列的报文会优先发送，但为了防止低优先级队列（AF、BE队列）得不到调度，EF队列以设置的带宽限速。当接口不拥塞时，EF队列可以占用AF、BE的空闲带宽。这样，属于EF队列的报文既可以获得空闲的带宽，又不会占用超出规定的带宽，保护了其他报文的应得带宽。

  设备除了提供普通的EF队列，还支持一种特殊的EF队列—LLQ队列。LLQ队列较EF队列而言，时延更低。这为时延敏感的应用（如VoIP业务）提供了良好的服务质量保证。

- AF队列

  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列的时候，按用户为各类报文设定的带宽将报文出队列发送，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。

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

  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。

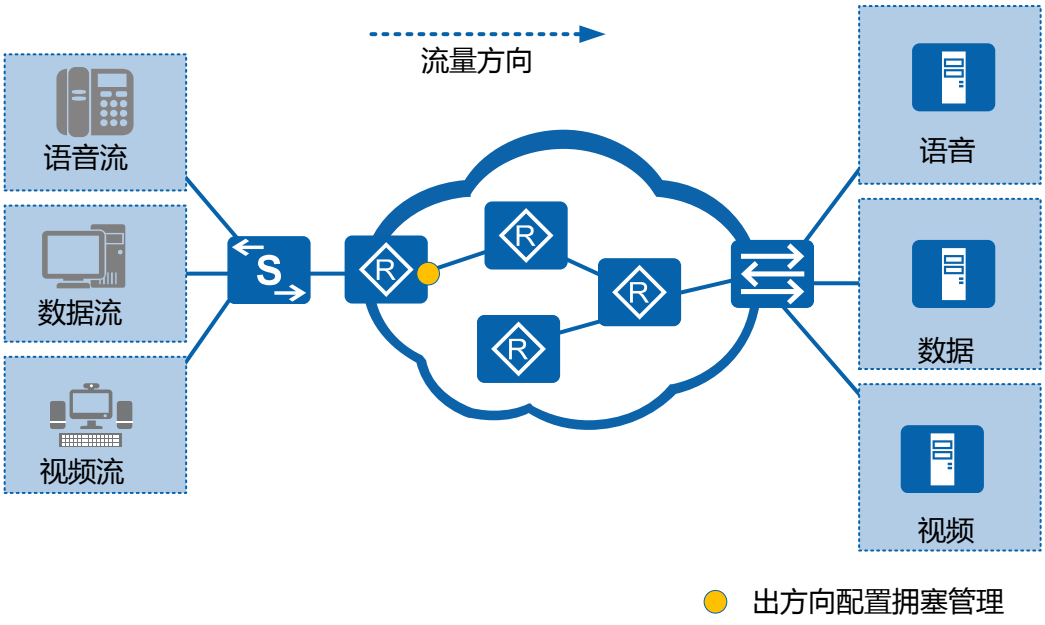
4.3 应用场景

拥塞管理的应用

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

在企业网络中，当共享同一网络的多种业务竞争相同的资源（带宽，缓冲区等）时可能会产生拥塞，高优先级业务无法得到保证。此时可以通过优先级映射的结果将报文送入不同的队列，如图4-11所示，在设备出方向为不同的队列配置不同的调度方式，可以达到对不同业务进行差分服务的目的。

图 4-11 拥塞管理应用组网图

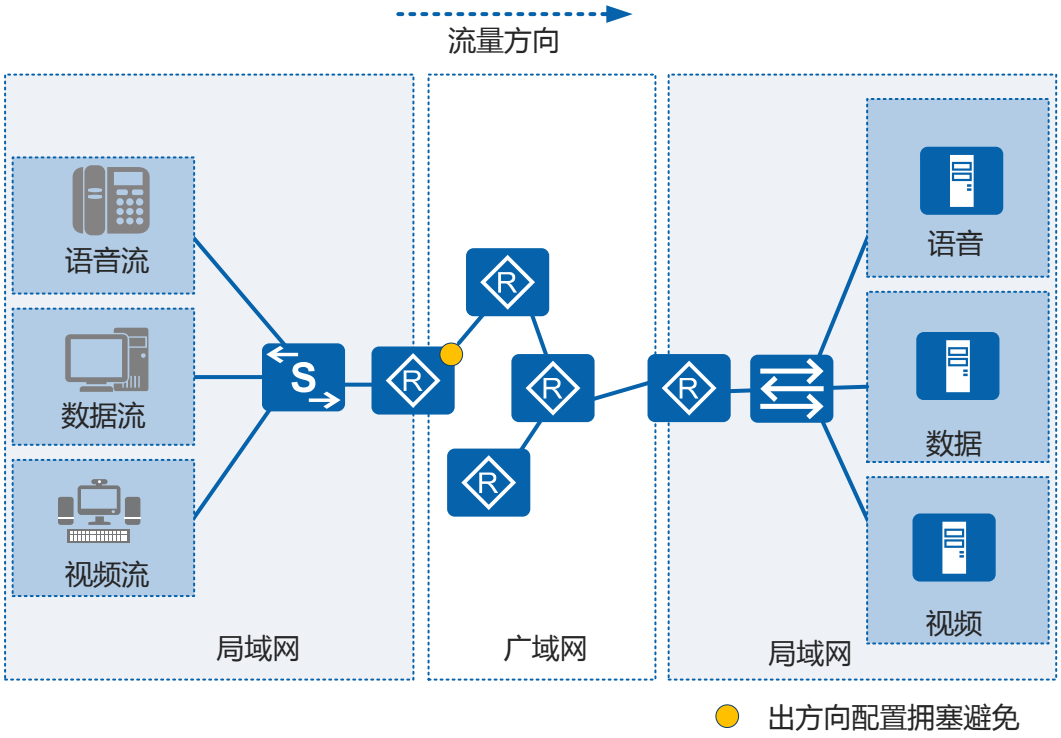


拥塞避免的应用

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

各地用户有可能向同一台服务器上传数据，因此用户与服务器之间的通信会经过广域网，由于广域网带宽小于局域网的带宽，位于广域网和局域网之间的边缘设备将可能发生拥塞，此时可以通过配置拥塞避免，主动丢弃优先级较低的报文（比如数据报文等），减少网络的拥塞，保证高优先级业务正常运行，如图4-12所示。

图 4-12 拥塞避免应用组网图



4.4 缺省配置

拥塞管理和拥塞避免缺省配置介绍了拥塞管理和拥塞避免常用参数的缺省配置。

表 4-2 拥塞管理和拥塞避免缺省配置

参数	缺省值
调度方式	● LAN接口：WRR ● 以太WAN接口（AR3600系列除外）：不采用队列调度模式 ● 其他WAN接口：WFQ
队列权重	10

4.5 配置拥塞管理

配置拥塞管理后，当网络中发生拥塞时，设备将按照配置的调度策略决定报文转发时的处理次序，确保高优先级业务优先发送。

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

配置流程

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。请根据需要选择其中一项进行配置。

4.5.1 配置基于队列的拥塞管理

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。设备上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。各接口支持的调度模式如**表4-3**所示。

表 4-3 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系列设备上的二层FE接口不支持DRR调度模式，仅支持PQ、WRR和PQ+WRR模式。 ● AR160（AR161、AR161W、AR169、AR169EW、AR169CVW、AR169CVW-4B4S、AR169EGW-L、AR161G-L、AR161EW、AR161EW-M1、AR161G-Lc、AR161G-U、AR169G-L、AR169W-P-M9、AR169RW-P-M9和AR169-P-M9除外）系列设备上的二层GE接口不支持DRR调度模式，仅支持PQ、WRR和PQ+WRR模式。 ● AR1200系列（AR1220E、AR1220EV和AR1220EVW除外）主控板上的FE接口不支持DRR调度模式，仅支持PQ、WRR和PQ+WRR模式。 ● V200R008C50及以后版本，二层VE接口仅支持WAN接口的调度模式，即PQ、WFQ和PQ+WFQ。
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，请选择执行下列命令，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。
- V200R008C50及以后版本，对于二层VE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。

- 对于其他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（除二层VE接口）所有队列均采用WRR调度模式；其他WAN侧口和二层VE接口所有队列默认均采用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。

说明

- 执行**queue length**命令配置了队列长度的队列模板，不能应用到4ES2GP-S、4ES2G-S、9ES2单板的接口。
- 执行**queue length**命令配置了队列长度的队列模板，不能应用到AR150&AR200系列设备的二层FE接口。
- 执行**queue length**命令配置了队列长度的队列模板，不能应用到AR100&AR120&AR160系列设备的二层GE接口。
- 执行**queue length**命令配置了队列长度的队列模板，不能应用到AR1200系列设备主控板上的FE接口。
- 当队列模板应用到设备的LAN接口上时，实际支持配置的最大可存储报文数范围为1～25。

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

- 执行**queue weight**命令配置了队列权重的队列模板，不能应用到4ES2GP-S、4ES2G-S、9ES2单板的接口。
- 执行**queue weight**命令配置了队列权重的队列模板，不能应用到AR150&AR200系列设备的二层FE接口。
- 执行**queue weight**命令配置了队列权重的队列模板，不能应用到AR100&AR120&AR160系列设备的二层GE接口。
- 执行**queue weight**命令配置了队列权重的队列模板，不能应用到AR1200系列设备主控板上的FE接口。

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

4.5.2 配置 MQC 实现拥塞管理

背景信息

设备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。而且当AF或BE队列

有空闲带宽时，EF队列可以对空闲带宽进行占用。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。

设备除了提供普通的EF队列，还支持一种特殊的EF队列—LLQ队列。LLQ队列较EF队列而言，时延更低。

- 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。

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:
  - 如果AF队列以百分比方式配置可确保的最小带宽：
    - 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可用带宽的99%。
    - 当AF队列和EF队列带宽之和占接口可用带宽的比列小于90%时，系统默认为BE队列分配的带宽为接口可用带宽的10%。
    - 当AF队列和EF队列带宽之和占接口可用带宽的比例大于90%时（如A%），系统默认为BE队列分配的带宽为100%-A%。
    - 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）。
  - 如果AF队列以带宽值方式配置可确保的最小带宽，则AF队列和BE队列固定按照9：1的比列分享剩余带宽（剩余带宽即可用带宽减去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4-4所示：

表 4-4 拥塞管理配置参数示例

接口可用带宽	用户配置
100Mbit/s	EF队列：最小带宽为接口带宽的50%
	AF队列：最小带宽为30Mbit/s
	BE队列：**default-class**与BE队列关联使用，系统默认为其分配带宽为AF队列带宽的1/9

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100Mbit/s×50%=50Mbit/s
- 剩余带宽为100Mbit/s－50Mbit/s=50Mbit/s

- AF队列和BE队列按照9：1的权重分享剩余带宽：
  - AF队列带宽为50Mbit/s×[9/(9+1)]=45Mbit/s
  - BE队列带宽为50Mbit/s×[1/(9+1)]=5Mbit/s

主接口或子接口上配置的基于流的拥塞管理（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）	是否可以配置流量整形（qos gts或qos gts adaptation-profile）
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

说明

V200R008C30及以前版本，基于流的拥塞管理只能配置在设备的WAN接口上，LAN接口不支持此配置。

V200R008C50及以后版本，基于流的拥塞管理只能配置在设备的WAN接口和二层VE接口上。

操作步骤

1. 配置流分类
   a. 执行命令**system-view**，进入系统视图。
   b. 执行命令**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]，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”，指定该逻辑关系后：
      - 当流分类中有ACL规则时，报文必须匹配其中一条ACL规则以及所有非ACL规则才属于该类。
      - 当流分类中没有ACL规则时，则报文必须匹配所有非ACL规则才属于该类。

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

      缺省情况下，流分类中各规则之间的关系为“逻辑或”。
   c. 请根据实际情况配置流分类中的匹配规则。

匹配规则	命令
外层VLAN ID	**if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*]
QinQ报文内层VLAN ID	**if-match cvlan-id** *start-vlan-id* [**to** *end-vlan-id*]
VLAN报文802.1p优先级	**if-match 8021p** *8021p-value* &<1-8>

匹配规则	命令
QinQ报文内层VLAN的802.1p优先级	**if-match cvlan-8021p** *8021p-value* &<1-8>
MPLS报文EXP优先级（AR1200&AR2200&AR3200&AR3600系列）	**if-match mpls-exp** *exp-value* &<1-8>
目的MAC地址	**if-match destination-mac** *mac-address* [**mac-address-mask** *mac-address-mask*]
源MAC地址	**if-match source-mac** *mac-address* [**mac-address-mask** *mac-address-mask*]
FR报文中的DLCI信息	**if-match dlci** *start-dlci-number* [**to** *end-dlci-number*]
FR报文中的DE标志位	**if-match fr-de**
以太网帧头中协议类型字段	**if-match l2-protocol** { **arp** | **ip** | **mpls** | **rarp** | *protocol-value* }
所有报文	**if-match any**
IP报文的DSCP优先级	**if-match** [**ipv6**] **dscp** *dscp-value* &<1-8> **说明** 如果流策略中配置了匹配DSCP，则SAE220（WSIC）和SAE550（XSIC）单板不支持**redirect ip-nexthop** *ip-address* **post-nat**动作。
IP报文的IP优先级	**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 [ipv6] dscp**和**if-match ip-precedence**。
报文三层协议类型	**if-match protocol** { **ip** | **ipv6** }
指定QoS group索引的IPSec报文	**if-match qos-group** *qos-group-value*
IPv4报文长度	**if-match packet-length** *min-length* [**to** *max-length*]
ATM报文中的PVC信息	**if-match pvc** *vpi-number*/*vci-number*
RTP端口号	**if-match rtp start-port** *start-port-number* **end-port** *end-port-number*
TCP报文SYN Flag	**if-match tcp syn-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** }*
入接口	**if-match inbound-interface** *interface-type interface-number*
出接口	**if-match outbound-interface Cellular** *interface-number:channel*

匹配规则	命令
ACL规则	**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。 ● 当使用ACL作为流分类规则匹配源IP地址时，通过在接口下的**qos pre-nat**配置NAT预分类功能，可以将NAT转换前的私网IP地址信息携带到出接口，即可实现基于私网IP地址的分类，从而对来自不同私网IP地址的报文提供差分服务。
ACL6规则	**if-match ipv6 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。 ● 当使用ACL作为流分类规则匹配源IP地址时，通过在接口下的**qos pre-nat**配置NAT预分类功能，可以将NAT转换前的私网IP地址信息携带到出接口，即可实现基于私网IP地址的分类，从而对来自不同私网IP地址的报文提供差分服务。
应用协议	**if-match application** *application-name* [**user-set** *user-set-name*] [**time-range** *time-name*] **说明** 定义基于应用协议的匹配规则前，必须使能SA功能并加载特征库。
SA协议组	**if-match category** *category-name* [**user-set** *user-set-name*] [**time-range** *time-name*] **说明** ● 定义基于应用协议的匹配规则前，必须使能SA功能并加载特征库。
用户组	**if-match user-set** *user-set-name* [**time-range** *time-range-name*]

d. 执行命令**quit**，退出流分类视图。

2. 配置流行为

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

b. 请根据实际需要，选择执行下列命令，配置队列的调度方式：

- 执行命令**queue af bandwidth** [**remaining**] { *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，并配置允许的最小带宽。
- 执行命令**queue llq bandwidth** { *bandwidth* [**cbs** *cbs-value*] | **pct** *percentage* [**cbs** *cbs-value*] }，配置符合要求的某一类报文进入LLQ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。

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

说明

不允许为LLQ队列配置队列的最大长度。

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

e. 执行命令**quit**，退出流行为视图。

f. 执行命令**quit**，退出系统视图。

3. 配置流策略

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**traffic policy** *policy-name*，创建一个流策略并进入流策略视图，或进入已存在的流策略视图。

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

d. 执行命令**quit**，退出流策略视图。

e. 执行命令**quit**，退出系统视图。

4. 应用流策略

- 在接口下应用流策略

i. 执行命令**system-view**，进入系统视图。

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

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

- 在安全域间应用流策略

说明

仅AR100&AR120&AR150&AR160&AR200系列支持此步骤。

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**firewall interzone** *zone-name1 zone-name2*，创建安全域间并进入安全域间视图。

缺省情况下，未创建安全域间。

创建安全域间必须指定两个已存在的安全区域。

iii. 执行命令**traffic-policy** *policy-name*，在安全域间绑定流策略。

缺省情况下，安全域间没有绑定流策略。

- 在BD下应用流策略

说明

仅在V200R008C30及之后版本，AR100&AR120&AR150&AR160&AR200&AR1200系列和AR2220E支持此步骤。

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**bridge-domain** *bd-id*，创建广播域BD（Bridge Domain）并进入BD视图。

缺省情况下，没有创建广播域BD。

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

缺省情况下，BD下没有应用任何流策略。

4.5.3 检查配置结果

操作步骤

- 检查基于队列的拥塞管理配置结果
  - 在应用了队列模板的接口下进入接口视图，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 applied-record** *policy-name*，查看指定拥塞管理策略的应用记录信息。

----结束

4.6 配置拥塞避免

配置拥塞避免后，设备将根据配置的丢弃模板主动丢弃超出流量范围的报文，以调整网络流量，解除网络过载。

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
- 配置拥塞管理

配置流程

基于队列的拥塞避免与基于流分类的拥塞避免互斥，不可同时配置。请根据需要选择其中一项进行配置。

4.6.1 配置基于队列的 WRED

背景信息

说明

V200R008C30及以前版本，LAN侧接口板不支持WRED。V200R008C50及以后版本，二层VE接口支持WRED。

丢弃模板是队列各优先级WRED参数的集合，将丢弃模板在队列模板中绑定后，应用到接口上，可以实现对接口上绑定丢弃模板的队列的拥塞避免。

设备支持基于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，如DSCP优先级0～7对应IP优先级0，DSCP优先级8～15对应IP优先级1，以此类推。

可见，基于DSCP优先级配置WRED参数可以对流量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

V200R008C30及以前版本，设备仅支持为WAN接口的队列模板中调度模式为WFQ的队列绑定丢弃模板。

V200R008C50及以后版本，设备支持为WAN接口和二层VE+接口的队列模板中调度模式为WFQ的队列绑定丢弃模板。

对于队列中的MPLS报文，AR1200系列、AR2200系列或AR3200&AR3600系列按照报文中EXP优先级的8倍查找DSCP丢弃模板的WRED参数，进行丢弃。例如当报文的EXP优先级为2，则在丢弃模板中查找DSCP优先级为16的WRED参数，按照此参数进行丢弃。

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*，在接口或子接口下应用队列模板。

----结束

4.6.2 配置 MQC 实现拥塞避免

背景信息

丢弃模板是队列各优先级WRED参数的集合。丢弃模板在流行为中绑定后，将流行为和对应的流分类在流策略下进行关联，并将此流策略应用到接口上，可以实现对匹配流分类规则的流量的拥塞避免。

设备支持基于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，如DSCP优先级0～7对应IP优先级0，DSCP优先级8～15对应IP优先级1，以此类推。

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

V200R008C30及以前版本，拥塞避免只能配置在设备的WAN接口上，LAN接口不支持此配置。

V200R008C50及以后版本，拥塞避免可以配置在设备的WAN接口和二层VE接口上，其他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MQC实现拥塞管理。

对于队列中的MPLS报文，AR1200系列、AR2200系列或AR3200&AR3600系列按照报文中EXP优先级的8倍查找DSCP丢弃模板的WRED参数，进行丢弃。例如当报文的EXP优先级为2，则在丢弃模板中查找DSCP优先级为16的WRED参数，按照此参数进行丢弃。

操作步骤

1. 配置丢弃模板
   a. 执行命令**system-view**，进入系统视图。
   b. 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。
   c. （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。
   d. 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。
   e. 执行命令**quit**，退出丢弃模板视图。
   f. 执行命令**quit**，退出系统视图。

2. 配置流分类

   a. 执行命令**system-view**，进入系统视图。

   b. 执行命令**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]，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”，指定该逻辑关系后：

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

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

      缺省情况下，流分类中各规则之间的关系为“逻辑或”。

   c. 请根据实际情况配置流分类中的匹配规则。

匹配规则	命令
外层VLAN ID	**if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*]
QinQ报文内层VLAN ID	**if-match cvlan-id** *start-vlan-id* [**to** *end-vlan-id*]
VLAN报文802.1p优先级	**if-match 8021p** *8021p-value* &<1-8>
QinQ报文内层VLAN的802.1p优先级	**if-match cvlan-8021p** *8021p-value* &<1-8>
MPLS报文EXP优先级（AR1200&AR2200&AR3200&AR3600系列）	**if-match mpls-exp** *exp-value* &<1-8>
目的MAC地址	**if-match destination-mac** *mac-address* [**mac-address-mask** *mac-address-mask*]
源MAC地址	**if-match source-mac** *mac-address* [**mac-address-mask** *mac-address-mask*]
FR报文中的DLCI信息	**if-match dlci** *start-dlci-number* [**to** *end-dlci-number*]
FR报文中的DE标志位	**if-match fr-de**
以太网帧头中协议类型字段	**if-match l2-protocol** { **arp** | **ip** | **mpls** | **rarp** | *protocol-value* }
所有报文	**if-match any**
IP报文的DSCP优先级	**if-match** [**ipv6**] **dscp** *dscp-value* &<1-8> **说明** 如果流策略中配置了匹配DSCP，则SAE220（WSIC）和SAE550（XSIC）单板不支持**redirect ip-nexthop** *ip-address* **post-nat**动作。

匹配规则	命令
IP报文的IP优先级	**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 [ipv6] dscp**和**if-match ip-precedence**。
报文三层协议类型	**if-match protocol** { **ip** | **ipv6** }
指定QoS group索引的IPSec报文	**if-match qos-group** *qos-group-value*
IPv4报文长度	**if-match packet-length** *min-length* [**to** *max-length*]
ATM报文中的PVC信息	**if-match pvc** *vpi-number/vci-number*
RTP端口号	**if-match rtp start-port** *start-port-number* **end-port** *end-port-number*
TCP报文SYN Flag	**if-match tcp syn-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** }*
入接口	**if-match inbound-interface** *interface-type interface-number*
出接口	**if-match outbound-interface Cellular** *interface-number:channel*
ACL规则	**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。 ● 当使用ACL作为流分类规则匹配源IP地址时，通过在接口下的**qos pre-nat**配置NAT预分类功能，可以将NAT转换前的私网IP地址信息携带到出接口，即可实现基于私网IP地址的分类，从而对来自不同私网IP地址的报文提供差分服务。
ACL6规则	**if-match ipv6 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。 ● 当使用ACL作为流分类规则匹配源IP地址时，通过在接口下的**qos pre-nat**配置NAT预分类功能，可以将NAT转换前的私网IP地址信息携带到出接口，即可实现基于私网IP地址的分类，从而对来自不同私网IP地址的报文提供差分服务。
应用协议	**if-match application** *application-name* [**user-set** *user-set-name*] [**time-range** *time-name*] **说明** 定义基于应用协议的匹配规则前，必须使能SA功能并加载特征库。

匹配规则	命令
SA协议组	**if-match category** *category-name* [**user-set** *user-set-name*] [**time-range** *time-name*] **说明** ● 定义基于应用协议的匹配规则前，必须使能SA功能并加载特征库。
用户组	**if-match user-set** *user-set-name* [**time-range** *time-range-name*]

d. 执行命令**quit**，退出流分类视图。

3. 配置流行为

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

说明

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

b. 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。

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

d. 执行命令**quit**，退出流行为视图。

e. 执行命令**quit**，退出系统视图。

4. 配置流策略

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**traffic policy** *policy-name*，创建一个流策略并进入流策略视图，或进入已存在的流策略视图。

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

d. 执行命令**quit**，退出流策略视图。

e. 执行命令**quit**，退出系统视图。

5. 应用流策略

- 在接口下应用流策略

i. 执行命令**system-view**，进入系统视图。

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

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

- 在安全域间应用流策略

说明

仅AR100&AR120&AR150&AR160&AR200系列支持此步骤。

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**firewall interzone** *zone-name1 zone-name2*，创建安全域间并进入安全域间视图。

缺省情况下，未创建安全域间。

创建安全域间必须指定两个已存在的安全区域。

iii. 执行命令**traffic-policy** *policy-name*，在安全域间绑定流策略。

缺省情况下，安全域间没有绑定流策略。

- 在BD下应用流策略

说明

仅在V200R008C30及之后版本，AR100&AR120&AR150&AR160&AR200&AR1200系列和AR2220E支持此步骤。

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**bridge-domain** *bd-id*，创建广播域BD（Bridge Domain）并进入BD视图。

缺省情况下，没有创建广播域BD。

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

缺省情况下，BD下没有应用任何流策略。

4.6.3 检查配置结果

操作步骤

- 检查基于队列的拥塞避免配置结果
  - 在绑定了队列模板的接口下，进入接口视图，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 applied-record** *policy-name*，查看指定流量整形策略的应用记录信息。

----结束

4.7 配置举例

通过示例介绍如何应用拥塞管理和拥塞避免。配置示例中包括组网需求、配置注意事项、配置思路等。

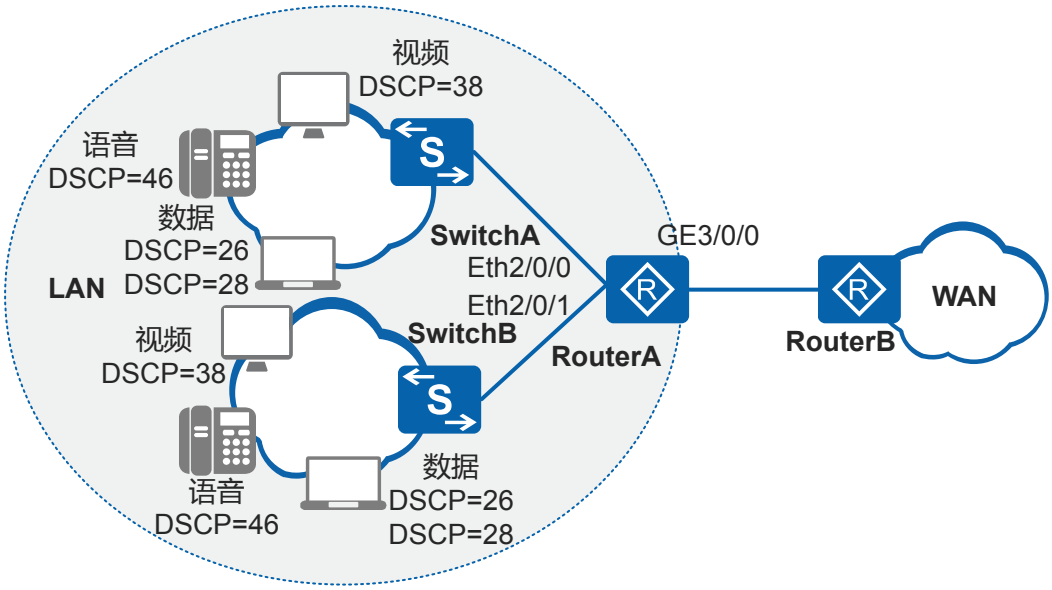
4.7.1 配置拥塞管理和拥塞避免综合示例

组网需求

如图4-13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Eth2/0/0和Eth2/0/1上，并通过RouterA的GE3/0/0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、af43、af32和af31，在RouterA上根据报文的DSCP优先级入队列，由于RouterA的接口Eth2/0/0和Eth2/0/1的速率大于接口GE3/0/0的速率，在接口GE3/0/0出方向处可能会发生拥塞。企业希望优先发送语音报文，对于视频和数据报文，确保优先级越小，获得发送的机会和获得的带宽越小，且被随机丢弃的概率越大，以调整网络流量，降低拥塞产生的影响。

图 4-13 配置拥塞管理和拥塞避免组网图



配置思路

采用拥塞管理和拥塞避免的方式来缓解拥塞，具体思路如下：

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，实现不同优先级的报文进入不同的队列。
3. 创建丢弃模板，并配置基于DSCP优先级的WRED参数，实现优先级越小，丢弃概率越大的丢弃策略。
4. 创建队列模板，配置语音报文采用PQ调度，视频和数据报文采用WFQ调度，实现对语音报文的优先发送，对视频、数据报文的按优先级调度。
5. 在队列模板中绑定丢弃模板，并把队列模板应用到RouterA与WAN侧网络连接的接口出方向上，实现拥塞避免和拥塞管理。

操作步骤

步骤1 创建VLAN并配置各接口

在RouterA上创建VLAN20和VLAN30。

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

配置接口Eth2/0/0和Eth2/0/1信任报文的DSCP优先级，均为Trunk类型端口，并将Eth2/0/0加入VLAN20，将Eth2/0/1加入VLAN30。

```
[RouterA] interface ethernet 2/0/0
[RouterA-Ethernet2/0/0] trust dscp
[RouterA-Ethernet2/0/0] port link-type trunk
[RouterA-Ethernet2/0/0] port trunk allow-pass vlan 20
[RouterA-Ethernet2/0/0] quit
[RouterA] interface ethernet 2/0/1
[RouterA-Ethernet2/0/1] trust dscp
[RouterA-Ethernet2/0/1] port link-type trunk
[RouterA-Ethernet2/0/1] port trunk allow-pass vlan 30
[RouterA-Ethernet2/0/1] 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VLANIF20和VLAN30，并为VLANIF20配置IP地址192.168.2.1/24，为VLANIF30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GE3/0/0的IP地址为192.168.4.1/24。

```
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] ip address 192.168.4.1 24
[RouterA-GigabitEthernet3/0/0] 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
[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
[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，配置各队列的调度模式。

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

说明

可通过**display qos map-table**命令查看当前RouterA的DSCP优先级与本地优先级之间的关系。报文将根据DSCP优先级映射的本地优先级值进入相应的队列。

步骤4 应用队列模板

在队列模板中绑定丢弃模板。

```
[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
```

把队列模板应用到RouterA的接口GE3/0/0上。

```
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] 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-GigabitEthernet3/0/0] display this
#
interface GigabitEthernet3/0/0
 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-GigabitEthernet3/0/0] 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 Ethernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 20
 trust dscp
#
interface Ethernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 30
 trust dscp
#
interface GigabitEthernet3/0/0
 ip address 192.168.4.1 255.255.255.0
 qos queue-profile queue-profile1
#
return
```

4.8 FAQ

介绍配置拥塞管理和拥塞避免的FAQ。

4.8.1 Tunnel 接口下的 af 队列、ef 队列如何计算带宽

由于Tunnel是虚拟接口，无法感知实际物理接口的带宽，因此规定：

- 如果接口未配置**qos gts**，可用带宽取值为1Gbit/s。
- 如果接口配置**qos gts**，可用带宽为**cir**的大小。

4.8.2 AR 上 LAN 侧和 WAN 侧单板，分别支持哪些调度模式

表 4-5 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系列设备上的二层FE接口不支持DRR调度模式，仅支持PQ、WRR和PQ+WRR模式。 ● AR160（AR161、AR161W、AR169、AR169EW、AR169CVW、AR169CVW-4B4S、AR169EGW-L、AR161G-L、AR161EW、AR161EW-M1、AR161G-Lc、AR161G-U、AR169G-L、AR169W-P-M9、AR169RW-P-M9和AR169-P-M9除外）系列设备上的二层GE接口不支持DRR调度模式，仅支持PQ、WRR和PQ+WRR模式。 ● AR1200系列（AR1220E、AR1220EV和AR1220EVW除外）主控板上的FE接口不支持DRR调度模式，仅支持PQ、WRR和PQ+WRR模式。 ● V200R008C50及以后版本，二层VE接口仅支持WAN接口的调度模式，即PQ、WFQ和PQ+WFQ。
WAN接口	● PQ ● WFQ ● PQ+WFQ

4.8.3 WFQ 队列权重的配置有何限制，是否要求各个队列权重值的总和是 100

WFQ每个队列的权重值的配置范围是1～100，通常配置队列权重总和为100，这样配置是为了计算方便，而各个队列的权重总和不要求一定是100。

每个队列所占带宽比例 = 本队列权重/所有队列权重和。

例如：假设当前接口中共有4个队列，其中3个队列的权重为10，1个队列的权重为50。那么，其中3个权重为10的队列获得的带宽比例均为10/80，权重为50的队列获得的带宽比例为50/80。

4.8.4 配置队列长度有哪些影响

队列长度越长，可以缓存的报文就越多，但引入的额外延迟也就要多。

对于网络中间歇性的拥塞，缓存更多的报文可以避免不必要丢弃，但是如果长期出现拥塞，增加队列的长度已经无法解决问题，就需要增加带宽。

4.8.5 配置丢弃模板有何用途

丢弃模板有如下两种用途：

- 缺省情况下，AR采用尾部丢弃，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，配置队列上丢弃模板，使用WRED随机丢弃策略可以很好的避免这种现象。
- 通过丢弃模板还根据不同优先级配置不同的丢弃概率，使得低优先级的报文优先被丢弃，保证用户对于高优先级、低延迟业务的服务要求。

4.8.6 EF 队列在什么情况下会抢占空闲带宽

当设备接口流量不拥塞且AF或BE队列有空闲带宽时，EF队列可以对空闲带宽进行占用。

主控板为SRU80、SRU200、SRU200E、SRU400或SRUX5时，设备的以太接口和POS接口不支持EF队列抢占空闲带宽功能。

4.9 参考信息

介绍QoS特性的相关参考资料。

文档	描述	备注
RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	-
RFC 2475	An Architecture for Differentiated Services	-
RFC 2597	Assured Forwarding PHB Group	-
RFC 2598	An Expedited Forwarding PHB	-
RFC 2697	A Single Rate Three Color Marker	-
RFC 2698	A Two Rate Three Color Marker	-

5 报文过滤配置

关于本章

报文过滤配置介绍了报文过滤的作用、配置方法和配置示例。

5.1 报文过滤简介
通过MQC实现报文过滤。

5.2 应用场景
介绍报文过滤的应用场景。

5.3 配置报文过滤
介绍报文过滤详细的配置过程。

5.4 配置举例
通过示例介绍报文过滤。

5.5 参考信息

5.1 报文过滤简介

通过MQC实现报文过滤。

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

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

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

5.2 应用场景

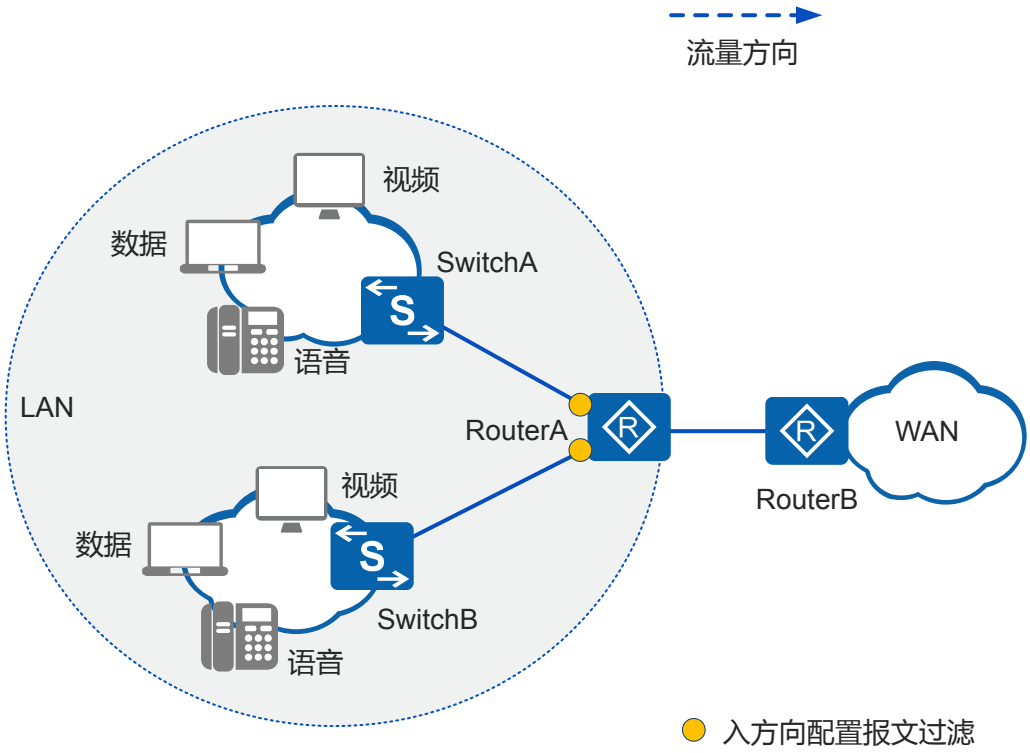
介绍报文过滤的应用场景。

报文过滤的应用

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

如图5-1所示，不同业务的报文在LAN侧使用802.1p优先级进行标识，用户希望能够在报文达到WAN侧之前对数据业务报文进行过滤，优先保证语音和视频业务的业务体验。

图 5-1 报文过滤应用组网图



5.3 配置报文过滤

介绍报文过滤详细的配置过程。

背景信息

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

操作步骤

1. 配置流分类
   a. 执行命令**system-view**，进入系统视图。
   b. 执行命令**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]，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”，指定该逻辑关系后：
      - 当流分类中有ACL规则时，报文必须匹配其中一条ACL规则以及所有非ACL规则才属于该类。
      - 当流分类中没有ACL规则时，则报文必须匹配所有非ACL规则才属于该类。

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

缺省情况下，流分类中各规则之间的关系为“逻辑或”。

c. 请根据实际情况配置流分类中的匹配规则。

匹配规则	命令
外层VLAN ID	**if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*]
QinQ报文内层VLAN ID	**if-match cvlan-id** *start-vlan-id* [**to** *end-vlan-id*]
VLAN报文802.1p优先级	**if-match 8021p** *8021p-value* &<1-8>
QinQ报文内层VLAN的802.1p优先级	**if-match cvlan-8021p** *8021p-value* &<1-8>
MPLS报文EXP优先级（AR1200&AR2200&AR3200&AR3600系列）	**if-match mpls-exp** *exp-value* &<1-8>
目的MAC地址	**if-match destination-mac** *mac-address* [**mac-address-mask** *mac-address-mask*]
源MAC地址	**if-match source-mac** *mac-address* [**mac-address-mask** *mac-address-mask*]
FR报文中的DLCI信息	**if-match dlci** *start-dlci-number* [**to** *end-dlci-number*]
FR报文中的DE标志位	**if-match fr-de**
以太网帧头中协议类型字段	**if-match l2-protocol** { **arp** | **ip** | **mpls** | **rarp** | *protocol-value* }
所有报文	**if-match any**
IP报文的DSCP优先级	**if-match** [**ipv6**] **dscp** *dscp-value* &<1-8> **说明** 如果流策略中配置了匹配DSCP，则SAE220（WSIC）和SAE550（XSIC）单板不支持**redirect ip-nexthop** *ip-address* **post-nat**动作。
IP报文的IP优先级	**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 [ipv6] dscp**和**if-match ip-precedence**。
报文三层协议类型	**if-match protocol** { **ip** | **ipv6** }
指定QoS group索引的IPSec报文	**if-match qos-group** *qos-group-value*
IPv4报文长度	**if-match packet-length** *min-length* [**to** *max-length*]

匹配规则	命令
ATM报文中的PVC信息	**if-match pvc** *vpi-number/vci-number*
RTP端口号	**if-match rtp start-port** *start-port-number* **end-port** *end-port-number*
TCP报文SYN Flag	**if-match tcp syn-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** }*
入接口	**if-match inbound-interface** *interface-type interface-number*
出接口	**if-match outbound-interface Cellular** *interface-number:channel*
ACL规则	**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。 ● 当使用ACL作为流分类规则匹配源IP地址时，通过在接口下的**qos pre-nat**配置NAT预分类功能，可以将NAT转换前的私网IP地址信息携带到出接口，即可实现基于私网IP地址的分类，从而对来自不同私网IP地址的报文提供差分服务。
ACL6规则	**if-match ipv6 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。 ● 当使用ACL作为流分类规则匹配源IP地址时，通过在接口下的**qos pre-nat**配置NAT预分类功能，可以将NAT转换前的私网IP地址信息携带到出接口，即可实现基于私网IP地址的分类，从而对来自不同私网IP地址的报文提供差分服务。
应用协议	**if-match application** *application-name* [**user-set** *user-set-name*] [**time-range** *time-name*] **说明** 定义基于应用协议的匹配规则前，必须使能SA功能并加载特征库。
SA协议组	**if-match category** *category-name* [**user-set** *user-set-name*] [**time-range** *time-name*] **说明** ● 定义基于应用协议的匹配规则前，必须使能SA功能并加载特征库。
用户组	**if-match user-set** *user-set-name* [**time-range** *time-range-name*]

d. 执行命令**quit**，退出流分类视图。

2. 配置流行为

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

b. 请根据实际需要进行如下配置：

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

说明

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

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

d. 执行命令**quit**，退出流行为视图。

e. 执行命令**quit**，退出系统视图。

3. 配置流策略

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**traffic policy** *policy-name*，创建一个流策略并进入流策略视图，或进入已存在的流策略视图。

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

d. 执行命令**quit**，退出流策略视图。

e. 执行命令**quit**，退出系统视图。

4. 应用流策略

- 在接口下应用流策略

i. 执行命令**system-view**，进入系统视图。

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

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

- 在安全域间应用流策略

说明

仅AR100&AR120&AR150&AR160&AR200系列支持此步骤。

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**firewall interzone** *zone-name1 zone-name2*，创建安全域间并进入安全域间视图。

缺省情况下，未创建安全域间。

创建安全域间必须指定两个已存在的安全区域。

iii. 执行命令**traffic-policy** *policy-name*，在安全域间绑定流策略。

缺省情况下，安全域间没有绑定流策略。

- 在BD下应用流策略

说明

仅在V200R008C30及之后版本，AR100&AR120&AR150&AR160&AR200&AR1200系列和AR2220E支持此步骤。

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**bridge-domain** *bd-id*，创建广播域BD（Bridge Domain）并进入BD视图。

缺省情况下，没有创建广播域BD。

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

缺省情况下，BD下没有应用任何流策略。

检查配置结果

- 执行命令**display traffic classifier user-defined** [*classifier-name*]，查看已配置的流分类信息。
- 执行命令**display traffic behavior** { **system-defined** | **user-defined** } [*behavior-name*]，查看已配置的流行为信息。
- 执行命令**display traffic policy user-defined** [*policy-name* [**classifier** *classifier-name*]]，查看流策略的配置信息。
- 执行命令**display traffic-policy applied-record** [*policy-name*]，查看指定流策略的应用记录。

5.4 配置举例

通过示例介绍报文过滤。

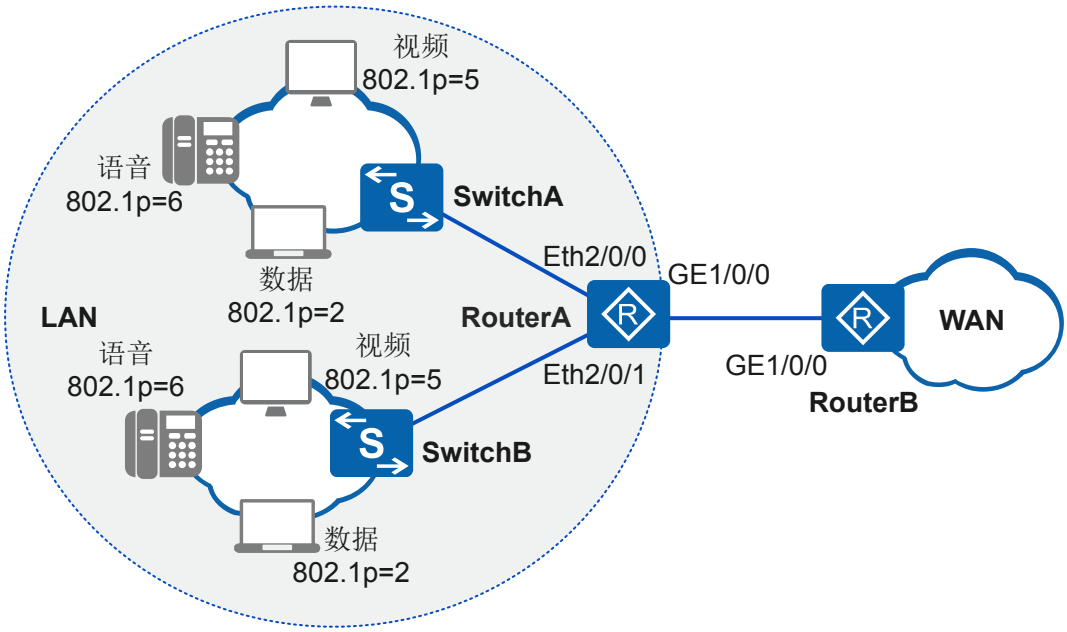
5.4.1 配置报文过滤示例

组网需求

如图5-2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的接口Eth2/0/0和Eth2/0/1上，并通过RouterA的GE1/0/0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，当报文从接口GE1/0/0到达WAN侧时，用户希望能够对数据业务报文进行过滤，优先保证语音和视频业务的业务体验。

图 5-2 配置报文过滤组网图



配置思路

采用包含禁止动作的流策略方式实现报文过滤，具体配置思路如下：

1. 配置各接口，实现企业用户能通过RouterA访问WAN侧网络。
2. 配置流分类，实现基于802.1p优先级对报文进行分类。
3. 配置流行为，实现对满足规则的报文进行禁止或允许动作。
4. 配置流策略，绑定上述流分类和流行为，并分别应用到接口Eth2/0/0和Eth2/0/1的入方向，实现报文过滤。

操作步骤

步骤1 创建VLAN并配置各接口

在RouterA上创建VLAN10和VLAN20。

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

配置RouterA上接口Eth2/0/0和Eth2/0/1为Trunk类型接口，并将Eth2/0/0加入VLAN10，将Eth2/0/1加入VLAN20。配置接口GE1/0/0的IP地址为192.168.4.1/24。

```
[RouterA] interface ethernet 2/0/0
[RouterA-Ethernet2/0/0] port link-type trunk
[RouterA-Ethernet2/0/0] port trunk allow-pass vlan 10
[RouterA-Ethernet2/0/0] quit
[RouterA] interface ethernet 2/0/1
[RouterA-Ethernet2/0/1] port link-type trunk
[RouterA-Ethernet2/0/1] port trunk allow-pass vlan 20
[RouterA-Ethernet2/0/1] quit
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 192.168.4.1 24
[RouterA-GigabitEthernet1/0/0] quit
```

说明

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

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

创建VLANIF10和VLANIF20，并为VLANIF10配置IP地址192.168.2.1/24，为VLANIF20配置IP地址192.168.3.1/24。

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

配置RouterB的接口GE1/0/0的IP地址为192.168.4.2/24。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ip address 192.168.4.2 24
[RouterB-GigabitEthernet1/0/0] quit
```

配置RouterB与LAN侧网络层互通。

```
[RouterB] ip route-static 192.168.2.0 255.255.255.0 192.168.4.1
[RouterB] ip route-static 192.168.3.0 255.255.255.0 192.168.4.1
```

说明

请配置SwitchA对应企业网内用户的缺省网关为192.168.2.1/24。

请配置SwitchB对应企业网内用户的缺省网关为192.168.3.1/24。

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上创建流行为b1，并配置禁止动作。

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

在RouterA上创建流行为b2和b3，并配置允许动作。

```
[RouterA] traffic behavior b2
[RouterA-behavior-b2] permit
[RouterA-behavior-b2] quit
[RouterA] traffic behavior b3
[RouterA-behavior-b3] permit
[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Eth2/0/0和Eth2/0/1的入方向上，对报文进行过滤。

```
[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 2/0/0
[RouterA-Ethernet2/0/0] traffic-policy p1 inbound
[RouterA-Ethernet2/0/0] quit
[RouterA] interface ethernet 2/0/1
[RouterA-Ethernet2/0/1] traffic-policy p1 inbound
[RouterA-Ethernet2/0/1] 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
```

查看流策略的应用信息。

```
<Router> display traffic-policy applied-record p1
----------------------------------------------
  Policy Name:   p1
  Policy Index:  0
     Classifier:c1     Behavior:b1
     Classifier:c2     Behavior:b2
     Classifier:c3     Behavior:b3
----------------------------------------------
 *interface Ethernet2/0/0
    traffic-policy p1 inbound
      slot 0    :  success
      slot 2    :  success
   Classifier: c1
    Operator: OR
    Rule(s) :
     if-match 8021p 2
     Behavior: b1
      Deny
   Classifier: c2
    Operator: OR
    Rule(s) :
     if-match 8021p 5
     Behavior: b2
   Classifier: c3
    Operator: OR
    Rule(s) :
     if-match 8021p 6
     Behavior: b3
 *interface Ethernet2/0/1
    traffic-policy p1 inbound
      slot 0    :  success
      slot 2    :  success
   Classifier: c1
    Operator: OR
    Rule(s) :
     if-match 8021p 2
     Behavior: b1
```

```
    Deny
  Classifier: c2
   Operator: OR
   Rule(s) :
    if-match 8021p 5
    Behavior: b2
  Classifier: c3
   Operator: OR
   Rule(s) :
    if-match 8021p 6
    Behavior: b3
  Behavior: Be
     Assured Forwarding:
       Bandwidth 0 (Kbps)
-----------------------------------------------
 Policy total applied times: 2.
```

----结束

配置文件

- RouterA的配置文件

```
#
 sysname RouterA
#
vlan batch 10 20
#
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
traffic behavior b2
traffic behavior b1
 deny
#
traffic policy p1
 classifier c1 behavior b1
 classifier c2 behavior b2
 classifier c3 behavior b3
#
interface Vlanif10
 ip address 192.168.2.1 255.255.255.0
#
interface Vlanif20
 ip address 192.168.3.1 255.255.255.0
#
interface Ethernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 10
 traffic-policy p1 inbound
#
interface Ethernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
 traffic-policy p1 inbound
#
interface GigabitEthernet1/0/0
 ip address 192.168.4.1 255.255.255.0
#
return
```

- RouterB的配置文件

```
#
 sysname RouterB
```

```
#
interface GigabitEthernet1/0/0
 ip address 192.168.4.2 255.255.255.0
#
ip route-static 192.168.2.0 255.255.255.0 192.168.4.1
ip route-static 192.168.3.0 255.255.255.0 192.168.4.1
#
return
```

5.5 参考信息

介绍QoS特性的相关参考资料。

文档	描述	备注
RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	-
RFC 2475	An Architecture for Differentiated Services	-
RFC 2597	Assured Forwarding PHB Group	-
RFC 2598	An Expedited Forwarding PHB	-
RFC 2697	A Single Rate Three Color Marker	-
RFC 2698	A Two Rate Three Color Marker	-

6 HQoS 配置

关于本章

HQoS（Hierarchical Quality of Service）是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。

背景信息

说明

AR100&AR120系列（AR129CGVW-L除外）不支持HQoS。

6.1 HQoS概述
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，实现了精细化的QoS服务。

6.2 原理描述

6.3 应用场景

6.4 配置嵌套流策略
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。

6.5 （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，且不引入额外的延迟。

6.6 （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。

6.7 检查配置结果

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

6.9 参考信息

6.1 HQoS 概述

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，实现了精细化的QoS服务。

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，只要属于同一优先级的流量，就使用同一个端口队列，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，用户希望能够享受区分用户和用户业务的服务，以获得更好的服务质量。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，提供了精细化的服务质量保证。

6.2 原理描述

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，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。

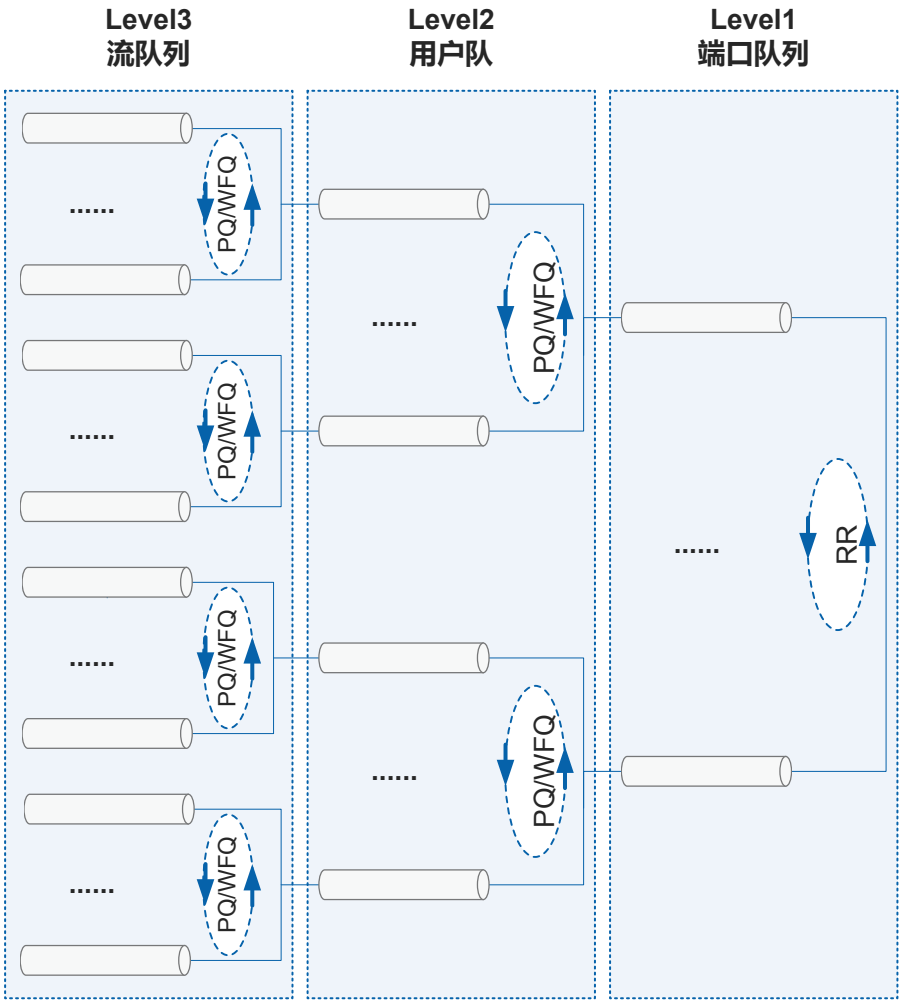
目前，越来越多的企业用户通过向运营商租用专线的方式来构建自己的企业网，不同企业之间，其业务侧重点和所需要的服务质量是有差别的。这就要求运营商能够依据不同企业的业务需求提供不同的调度策略和QoS保证。传统的QoS无法区分用户，所以无法对不同的企业用户提供有差别的队列调度服务。

随着网络用户数量的持续增长和网络业务的不断丰富，用户希望能够享受区分用户和用户业务的服务，以获得更好的服务质量。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

如图6-1所示，HQoS基于队列实现层次化调度，目前在设备上支持三级队列：Level3流队列（Flow Queue）、Level2用户队列（Subscriber Queue）、Level1接口队列（Port Queue）。三级队列以树状结构汇聚，流队列为叶子节点，接口队列为根结构。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。

图 6-1 HQoS 队列调度示意图



- 流队列

  每个用户的同类业务可以被认为是一个业务流，HQoS能够针对每个用户的不同业务流进行队列调度。流队列一般与业务类型相对应，包括EF、AF、BE等，用户可以配置流队列的调度方式。

- 用户队列

  来自同一用户的所有业务可以被认为是一个用户队列，HQoS可以使该用户队列下的所有业务共享一个用户队列的带宽。

- 接口队列

  每个接口一个队列，接口队列之间进行轮询调度（RR），用户仅可以配置基于接口的流量整形，且其调度方式不可配置。

HQoS 调度器

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。

设备提供了三级调度器，即流队列调度器、用户队列调度器和接口队列调度器。流队列调度器和用户队列调度器都支持PQ、WFQ、PQ+WFQ调度。接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

HQoS 整形器

整形器实现报文的缓存及限速功能。设备支持三级整形器，即流队列整形器、用户队列整形器和接口队列整形器。报文进入设备后先缓存到队列，再限速从队列发送报文，整形器配合限速算法可以保证承诺速率并限制最大速率。

HQoS 丢弃器

丢弃器在报文入队列之前将根据丢弃策略丢弃报文。HQoS支持的3种队列支持不同的丢弃方式：

- 接口队列：尾部丢弃
- 用户队列：尾部丢弃
- 流队列：尾部丢弃和WRED

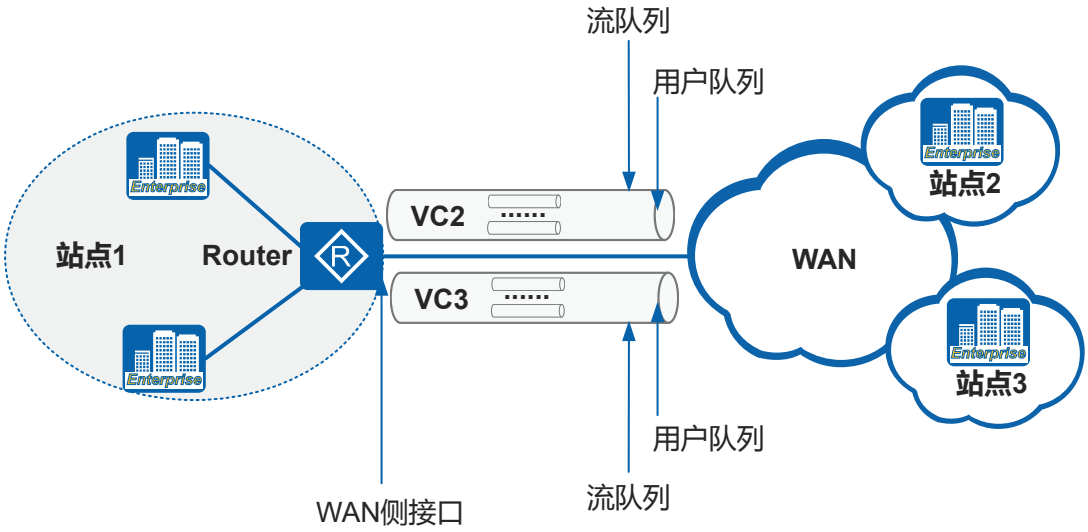
6.3 应用场景

HQoS 的应用

图6-2所示为企业网的典型应用组网，站点1为总部，站点2和站点3为2个子部门，子部门与总部通过两条子链路连接。各部门都有语音、视频、数据等业务流。

要求各部门有各自的保证带宽，并且能共享接口的最大带宽；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 6-2 HQoS 典型应用组网图



在设备WAN侧接口的出方向上，可以通过部署HQoS来实现上述需求。在接口上应用嵌套流策略，其中，父策略的流分类区分不同的用户，即用户队列；子策略的流分类区分不同的业务类型，即流队列。同时，CBQ提供的EF队列可以实现语音报文的优先发送，AF队列可以实现带宽保证。

6.4 配置嵌套流策略

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。

前置任务

在配置嵌套流策略之前，需要完成以下任务：

- 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。

6.4.1 配置子流策略

背景信息

子流策略用来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。

在主接口上配置嵌套流策略时，子策略的流行为中支持配置流量整形、自适应流量整形、拥塞管理或拥塞避免。

在子接口上配置嵌套流策略时，仅支持以下两种组合：

- 在子策略的流行为中配置除流量整形、自适应流量整形、拥塞管理和拥塞避免以外的QoS动作，则父策略的流行为中仅支持配置流量整形+子策略、流量整形+AF+子策略或EF+子策略。
- 在子策略的流行为中配置流量整形、拥塞管理或拥塞避免，则父策略的流分类中仅支持配置缺省分类**default-class**，且对应的流行为中仅支持配置流量整形。

操作步骤

步骤1 定义流分类

设备支持根据报文中的二层信息、报文中的三层信息、ACL等进行流分类。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**。

说明

若将嵌套流策略应用在接口或子接口的入方向，子策略流行为可以从以下三种中选择一种进行配置：

- CAR
- statistic
- CAR+statistic

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

6.4.2 配置父流策略

背景信息

父流策略用来区分网络中不同用户，配置父流策略前，必须已经完成子策略的配置。

在接口出方向上配置嵌套流策略时，父流策略的流行为可以从以下几种中选择一种进行配置：

- GTS+子策略：此时对用户的报文采取平均调度方式，接口带宽平均分配给用户。
- GTS+AF+子策略：通过配置AF，可以为不同的用户配置确保带宽占接口可用带宽的百分比。

  建议父策略中的每个用户都采用这种配置方式，这样可以通过配置AF为每一个用户带宽计算权重，为不同的用户分配不同的保证带宽。
- AF+子策略：通过配置AF，可以为不同的用户配置确保带宽占接口可用带宽的百分比。
- EF+子策略：当父策略绑定的是EF队列时，用户级队列是按照PQ调度的优先级进行调度的，可以优先保证优先级高的用户报文优先转发。

  必须先配置EF，再配置子策略。

在子接口出方向上配置嵌套流策略时，仅支持以下两种组合：

- 如果子策略的流行为中配置了除流量整形、自适应流量整形、拥塞管理和拥塞避免以外的QoS动作，则父策略的流行为中仅支持配置流量整形+子策略、流量整形+AF+子策略或EF+子策略。

- 如果子策略的流行为中配置了流量整形、拥塞管理或拥塞避免，则父策略的流分类中仅支持配置缺省分类**default-class**或**any**，且对应的流行为中仅支持配置流量整形。

在接口或子接口入方向上配置嵌套流策略时，父流策略的流行为可以从以下三种中选择一种进行配置：

- CAR+子策略
- statistic+子策略
- CAR+statistic+子策略

说明

父策略的流行为中配置的子策略不能是父策略本身。

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

- 在主接口出方向上配置嵌套流策略时，请根据组网需要，选择以下动作进行配置：
  - 配置GTS+子策略
    i. 执行命令**system-view**，进入系统视图。
    ii. 执行命令**traffic behavior** *behavior-name*，创建一个流行为，并进入流行为视图。
    iii. 执行命令**gts cir** { *cir-value* [**cbs** *cbs-value*] | **pct** *pct-value* } [**queue-length** *queue-length*]或**gts adaptation-profile** *adaptation-profile-name*，配置流量整形GTS动作。
    iv. 执行命令**traffic-policy** *policy-name*，在流行为中绑定子流策略。
    v. （可选）执行命令**statistic enable**，使能流量统计功能。
    vi. 执行命令**quit**，退出流行为视图。
  - 配置GTS+AF+子策略
    i. 执行命令**system-view**，进入系统视图。
    ii. 执行命令**traffic behavior** *behavior-name*，创建一个流行为，并进入流行为视图。
    iii. 执行命令**gts cir** { *cir-value* [**cbs** *cbs-value*] | **pct** *pct-value* } [**queue-length** *queue-length*]或**gts adaptation-profile** *adaptation-profile-name*，配置流量整形GTS动作。
    iv. 执行命令**queue af bandwidth** { *bandwidth* | **pct** *percentage* }，配置对某个用户确保转发和确保的最小带宽。
    v. 执行命令**traffic-policy** *policy-name*，在流行为中绑定子流策略。
    vi. （可选）执行命令**statistic enable**，使能流量统计功能。
    vii. 执行命令**quit**，退出流行为视图。
  - 配置AF+子策略

i. 执行命令**system-view**，进入系统视图。
ii. 执行命令**traffic behavior** *behavior-name*，创建一个流行为，并进入流行为视图。
iii. 执行命令**queue af bandwidth** { *bandwidth* | **pct** *percentage* }，配置对某个用户确保转发和确保的最小带宽。
iv. 执行命令**traffic-policy** *policy-name*，在流行为中绑定子流策略。
v. （可选）执行命令**statistic enable**，使能流量统计功能。
vi. 执行命令**quit**，退出流行为视图。

- 配置EF+子策略

i. 执行命令**system-view**，进入系统视图。
ii. 执行命令**traffic behavior** *behavior-name*，创建一个流行为，并进入流行为视图。
iii. 执行命令**queue ef bandwidth** { *bandwidth* [**cbs** *cbs-value*] | **pct** *percentage* [**cbs** *cbs-value*] }，配置对某个用户加速转发和确保的最小带宽。
iv. 执行命令**traffic-policy** *policy-name*，在流行为中绑定子流策略。
v. （可选）执行命令**statistic enable**，使能流量统计功能。
vi. 执行命令**quit**，退出流行为视图。

- 在子接口出方向上配置嵌套流策略时，请根据组网需要，结合“背景信息”中描述的配置原则，选择以下动作进行配置：
  - 配置流量整形+子策略

i. 执行命令**system-view**，进入系统视图。
ii. 执行命令**traffic behavior** *behavior-name*，创建一个流行为，并进入流行为视图。
iii. 执行命令**gts cir** { *cir-value* [**cbs** *cbs-value*] | **pct** *pct-value* } [**queue-length** *queue-length*]，配置流量整形动作。
iv. 执行命令**traffic-policy** *policy-name*，在流行为中绑定子流策略。
v. （可选）执行命令**statistic enable**，使能流量统计功能。
vi. 执行命令**quit**，退出流行为视图。

  - 配置流量整形+AF+子策略

i. 执行命令**system-view**，进入系统视图。
ii. 执行命令**traffic behavior** *behavior-name*，创建一个流行为，并进入流行为视图。
iii. 执行命令**gts cir** { *cir-value* [**cbs** *cbs-value*] | **pct** *pct-value* } [**queue-length** *queue-length*]，配置流量整形动作。
iv. 执行命令**queue af bandwidth** { *bandwidth* | **pct** *percentage* }，配置对某个用户确保转发和确保的最小带宽。
v. 执行命令**traffic-policy** *policy-name*，在流行为中绑定子流策略。
vi. （可选）执行命令**statistic enable**，使能流量统计功能。
vii. 执行命令**quit**，退出流行为视图。

  - 配置EF+子策略

i. 执行命令**system-view**，进入系统视图。
ii. 执行命令**traffic behavior** *behavior-name*，创建一个流行为，并进入流行为视图。

iii. 执行命令**queue ef bandwidth** { *bandwidth* [**cbs** *cbs-value*] | **pct** *percentage* [**cbs** *cbs-value*] }，配置对某个用户加速转发和确保的最小带宽。

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

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

vi. 执行命令**quit**，退出流行为视图。

- 配置流量整形

i. 执行命令**system-view**，进入系统视图。

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

iii. 执行命令**gts cir** { *cir-value* [**cbs** *cbs-value*] | **pct** *pct-value* } [**queue-length** *queue-length*]，配置流量整形动作。

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

v. 执行命令**quit**，退出流行为视图。

- 在接口或子接口入方向上配置嵌套流策略时：
  - 配置CAR+子策略

i. 执行命令**system-view**，进入系统视图。

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

iii. 对于AR100&AR120&AR150&AR160&AR200系列，执行命令**car cir** { *cir-value* | **pct** *cir-percentage* } [**pir** { *pir-value* | **pct** *pir-percentage* }] [**cbs** *cbs-value* **pbs** *pbs-value*] [**share**] [**mode** { **color-blind** | **color-aware** }] [**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*] }]，配置基于流的流量监管。

对于AR1200系列、AR2200系列、AR3200系列、AR3600系列，执行命令**car cir** { *cir-value* | **pct** *cir-percentage* } [**pir** { *pir-value* | **pct** *pir-percentage* }] [**cbs** *cbs-value* **pbs** *pbs-value*] [**share**] [**mode** { **color-blind** | **color-aware** }] [**green** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] [**yellow** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] [**red** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }]，配置基于流的流量监管。

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

v. 执行命令**quit**，退出流行为视图。

  - 配置statistic+子策略

i. 执行命令**system-view**，进入系统视图。

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

iii. 执行命令**statistic enable**，在流行为中使能流量统计功能。

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

v. 执行命令**quit**，退出流行为视图。

  - 配置CAR+statistic+子策略

i. 执行命令**system-view**，进入系统视图。

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

iii. 对于AR100&AR120&AR150&AR160&AR200系列，执行命令**car cir** { *cir-value* | **pct** *cir-percentage* } [**pir** { *pir-value* | **pct** *pir-percentage* }] [**cbs** *cbs-value* **pbs** *pbs-value*] [**share**] [**mode** { **color-blind** | **color-aware** }] [**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*] }]，配置基于流的流量监管。

对于AR1200系列、AR2200系列、AR3200&AR3600系列，执行命令**car cir** { *cir-value* | **pct** *cir-percentage* } [**pir** { *pir-value* | **pct** *pir-percentage* }] [**cbs** *cbs-value* **pbs** *pbs-value*] [**share**] [**mode** { **color-blind** | **color-aware** }] [**green** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] [**yellow** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] [**red** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }]，配置基于流的流量监管。

iv. 执行命令**statistic enable**，在流行为中使能流量统计功能。

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

vi. 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，即对同一类报文执行不同的动作，将会导致出错。

----结束

6.4.3 应用流策略

背景信息

将父流策略应用到接口或子接口上，实现精细化的QoS服务。

说明

V200R008C30及以前版本，设备仅支持在物理WAN接口或子接口上应用嵌套流策略。

V200R008C50及以后版本，设备支持在二层VE接口，物理WAN接口或子接口上应用嵌套流策略。

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* { **inbound** | **outbound** }，在接口或子接口上应用父流策略。

说明

- 子接口下应用嵌套流策略不能与主接口下基于队列的配置同时配置，例如主接口下配置流量整形、拥塞管理或拥塞避免。
- 当父策略和子策略中都有队列配置，例如流量整形、拥塞管理或拥塞避免，子接口下不能同时配置嵌套流策略和流量整形。
- 在子接口上应用嵌套策略时，父策略只能绑定一对流分类和流行为，且流分类只能使用默认流分类，即default-class。

----结束

6.5 （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，且不引入额外的延迟。

前置任务

配置接口的流量监管之前，需要完成以下任务：

- 完成嵌套流策略的配置

操作步骤

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

----结束

6.6 （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。

前置任务

配置接口的流量整形之前，需要完成以下任务：

- 完成嵌套流策略的配置

操作步骤

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

----结束

6.7 检查配置结果

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 applied-record** [*policy-name*]，查看指定流量整形策略的应用记录信息。
- 在配置了流量监管或流量整形的接口上，进入接口视图，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

6.8 配置举例

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

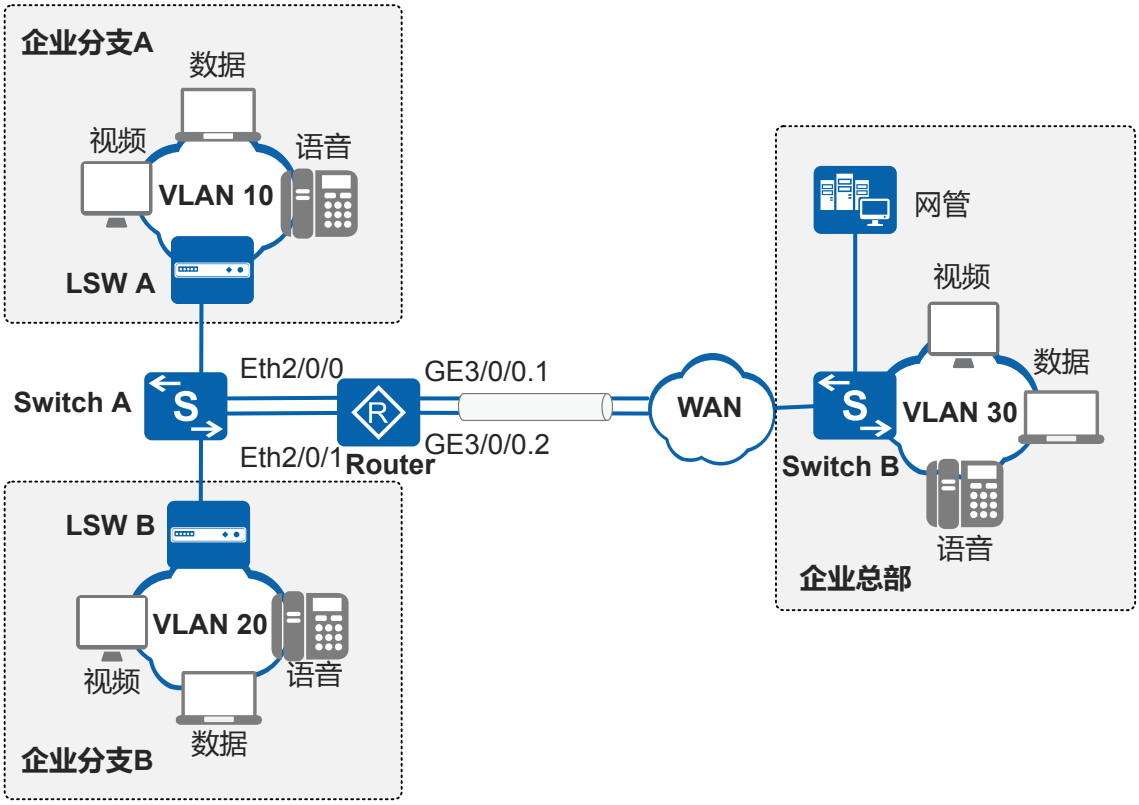
6.8.1 配置 HQoS 示例

组网需求

如图6-3所示，VLAN10和VLAN20是企业分支的两个部门，VLAN30是企业总部。企业分支通过交换机连接到Router，并通过Router的GE3/0/0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，企业内部还有网管的控制报文。

各类报文被Switch打上不同的DSCP优先级，语音、网管控制、视频和数据分别为ef、cs6、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，语音报文要保证低延时优先发送，网管控制报文要保证优先发送，视频、数据报文要保证带宽。

图 6-3 配置 HQoS 组网图



配置思路

采用流策略嵌套的方式配置HQoS，实现对不同业务的差分服务，具体思路如下：

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VLAN10和VLAN20的子流策略，基于DSCP优先级进行流分类，语音报文入LLQ队列，网管控制报文进入EF队列，视频和数据报文进入AF队列，并绑定丢弃模板。
3. 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。
4. 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。

操作步骤

步骤1 创建VLAN并配置各接口

在Router上创建VLAN10和VLAN20。

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

配置接口Eth2/0/0为Trunk类型端口，并将Eth2/0/0加入VLAN10。

```
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] port link-type trunk
[Router-Ethernet2/0/0] port trunk allow-pass vlan 10
[Router-Ethernet2/0/0] quit
```

配置接口Eth2/0/1为Trunk类型端口，并将Eth2/0/1加入VLAN20。

```
[Router] interface ethernet 2/0/1
[Router-Ethernet2/0/1] port link-type trunk
[Router-Ethernet2/0/1] port trunk allow-pass vlan 20
[Router-Ethernet2/0/1] 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VLANIF10和VLANIF20，并为VLANIF10配置IP地址192.168.1.1/24，为VLANIF20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GE3/0/0的IP地址为192.168.3.1/24。

```
[Router] interface gigabitethernet 3/0/0
[Router-GigabitEthernet3/0/0] ip address 192.168.3.1 24
[Router-GigabitEthernet3/0/0] quit
```

配置GE3/0/0.1的控制VLAN为10，封装方式为dot1q，IP地址为192.168.4.1/24，配置GE3/0/0.2的控制VLAN为20，封装方式为dot1q，IP地址为192.168.5.1/24。

```
[Router] interface gigabitethernet 3/0/0.1
[Router-GigabitEthernet3/0/0.1] ip address 192.168.4.1 24
[Router-GigabitEthernet3/0/0.1] dot1q termination vid 10
[Router-GigabitEthernet3/0/0.1] quit
[Router] interface gigabitethernet 3/0/0.2
[Router-GigabitEthernet3/0/0.2] ip address 192.168.5.1 24
[Router-GigabitEthernet3/0/0.2] dot1q termination vid 20
[Router-GigabitEthernet3/0/0.2] quit
```

步骤2 配置groupa和groupb的子流策略

在Router上创建流分类data、video、control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 control
[Router-classifier-control] if-match dscp cs6
[Router-classifier-control] 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、control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 45
[Router-behavior-data] drop-profile data
[Router-behavior-data] quit
[Router] traffic behavior video
[Router-behavior-video] queue af bandwidth pct 30
[Router-behavior-video] drop-profile video
[Router-behavior-video] quit
[Router] traffic behavior control
[Router-behavior-control] queue ef bandwidth pct 5
[Router-behavior-control] quit
[Router] traffic behavior voice
[Router-behavior-voice] queue llq bandwidth pct 15
[Router-behavior-voice] quit
```

在Router上定义groupa和groupb的子流策略。

```
[Router] traffic policy groupa-sub
[Router-trafficpolicy-groupa-sub] classifier voice  behavior voice
[Router-trafficpolicy-groupa-sub] classifier control  behavior control
[Router-trafficpolicy-groupa-sub] classifier video  behavior video
[Router-trafficpolicy-groupa-sub] classifier data  behavior  data
[Router-trafficpolicy-groupa-sub] quit
[Router] traffic policy groupb-sub
[Router-trafficpolicy-groupb-sub] classifier voice  behavior voice
[Router-trafficpolicy-groupb-sub] classifier control  behavior control
[Router-trafficpolicy-groupb-sub] classifier video  behavior video
[Router-trafficpolicy-groupb-sub] classifier data  behavior  data
[Router-trafficpolicy-groupb-sub] quit
```

步骤3 配置父流策略

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

```
[Router] traffic classifier groupa
[Router-classifier-groupa] if-match vlan-id 10
[Router-classifier-groupa] quit
[Router] traffic classifier groupb
[Router-classifier-groupb] if-match vlan-id 20
[Router-classifier-groupb] quit
```

在Router上创建流行为groupa和groupb，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 groupa
[Router-behavior-groupa] gts cir 20000 cbs 500000 queue-length 50
[Router-behavior-groupa] traffic-policy groupa-sub
[Router-behavior-groupa] quit
[Router] traffic behavior groupb
[Router-behavior-groupb] gts cir 30000 cbs 750000 queue-length 50
[Router-behavior-groupb] traffic-policy groupb-sub
[Router-behavior-groupb] quit
```

在Router上定义父流策略。

```
[Router] traffic policy enterprise
[Router-trafficpolicy-enterprise] classifier groupa behavior groupa
[Router-trafficpolicy-enterprise] classifier groupb behavior groupb
[Router-trafficpolicy-enterprise] quit
```

步骤4 应用父流策略

在Router的接口GE3/0/0出方向上应用父流策略。

```
[Router] interface gigabitethernet 3/0/0
[Router-GigabitEthernet3/0/0] traffic-policy enterprise outbound
```

步骤5 验证配置结果

查看Router接口的配置信息。

```
[Router-GigabitEthernet3/0/0] display this
#
interface GigabitEthernet3/0/0
 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-GigabitEthernet3/0/0] quit
[Router] display traffic-policy applied-record enterprise
-------------------------------------------------
  Policy Name:   enterprise
  Policy Index:  2
     Classifier:groupa     Behavior:groupa
     Classifier:groupb     Behavior:groupb
-------------------------------------------------
 *interface GigabitEthernet3/0/0
    traffic-policy enterprise outbound
      slot 3    :  success
      nest Policy :  groupa-sub
      slot 0    :  success
      nest Policy :  groupb-sub
      slot 0    :  success
   Classifier: groupa
    Operator: OR
    Rule(s) :
     if-match vlan-id 10
     Behavior: groupa
      General Traffic Shape:
        CIR 20000 (Kbps), CBS 500000 (byte)
        Queue length 50 (Packets)
      Nest Policy :  groupa-sub
       Classifier: voice
        Operator: OR
        Rule(s) :
         if-match dscp ef
         Behavior: voice
           Low-latency:
             Bandwidth 15 (%)
             Bandwidth 3000 (Kbps) CBS 75000 (Bytes)
       Classifier: control
        Operator: OR
        Rule(s) :
         if-match dscp cs6
         Behavior: control
           Expedited Forwarding:
             Bandwidth 5 (%)
             Bandwidth 1000 (Kbps) CBS 25000 (Bytes)
             Queue Length: 64 (Packets) 131072 (Bytes)
       Classifier: video
        Operator: OR
        Rule(s) :
         if-match dscp af21
         Behavior: video
           Assured Forwarding:
             Bandwidth 30 (%)
             Bandwidth 6000 (Kbps)
             Drop Method: WRED
             Drop-profile: video
```

```
     Classifier: data
      Operator: OR
      Rule(s) :
       if-match dscp af11
       Behavior: data
         Assured Forwarding:
           Bandwidth 45 (%)
           Bandwidth 9000 (Kbps)
           Drop Method: WRED
           Drop-profile: data
  Behavior: Be
     Assured Forwarding:
       Bandwidth 50000 (Kbps)
  Classifier: groupb
   Operator: OR
   Rule(s) :
    if-match vlan-id 20
    Behavior: groupb
     General Traffic Shape:
       CIR 30000 (Kbps), CBS 750000 (byte)
       Queue length 50 (Packets)
     Nest Policy :  groupa-sub
     Nest Policy :  groupb-sub
      Classifier: voice
       Operator: OR
       Rule(s) :
        if-match dscp ef
        Behavior: voice
          Low-latency:
            Bandwidth 15 (%)
            Bandwidth 4500 (Kbps) CBS 112500 (Bytes)
     Classifier: control
       Operator: OR
       Rule(s) :
        if-match dscp cs6
        Behavior: control
          Expedited Forwarding:
            Bandwidth 5 (%)
            Bandwidth 1500 (Kbps) CBS 37500 (Bytes)
            Queue Length: 64 (Packets) 131072 (Bytes)
     Classifier: video
       Operator: OR
       Rule(s) :
        if-match dscp af21
        Behavior: video
          Assured Forwarding:
            Bandwidth 30 (%)
            Bandwidth 9000 (Kbps)
            Drop Method: WRED
            Drop-profile: video
     Classifier: data
       Operator: OR
       Rule(s) :
        if-match dscp af11
        Behavior: data
          Assured Forwarding:
            Bandwidth 45 (%)
            Bandwidth 13500 (Kbps)
            Drop Method: WRED
            Drop-profile: data
  Behavior: Be
     Assured Forwarding:
       Bandwidth 50000 (Kbps)
-------------------------------------------------
  Policy total applied times: 1.
```

----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 control operator or
 if-match dscp cs6
traffic classifier groupb operator or
 if-match vlan-id 20
traffic classifier video operator or
 if-match dscp af21
traffic classifier groupa operator or
 if-match vlan-id 10
traffic classifier data operator or
 if-match dscp af11
traffic classifier voice operator or
 if-match dscp ef
#
traffic behavior control
 queue ef bandwidth pct 5
traffic behavior groupb
 gts cir 30000 cbs 750000 queue-length 50
 traffic-policy groupb-sub
traffic behavior video
 queue af bandwidth pct 30
 drop-profile video
traffic behavior groupa
 gts cir 20000 cbs 500000 queue-length 50
 traffic-policy groupa-sub
traffic behavior data
 queue af bandwidth pct 45
 drop-profile data
traffic behavior voice
 queue llq bandwidth pct 15
#
traffic policy groupa-sub
 classifier voice behavior voice
 classifier control behavior control
 classifier video behavior video
 classifier data behavior data
traffic policy enterprise
 classifier groupa behavior groupa
 classifier groupb behavior groupb
traffic policy groupb-sub
 classifier voice behavior voice
 classifier control behavior control
 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 Ethernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 10
#
```

```
interface Ethernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface GigabitEthernet3/0/0
 ip address 192.168.3.1 255.255.255.0
 traffic-policy enterprise outbound
#
interface GigabitEthernet3/0/0.1
 dot1q termination vid 10
 ip address 192.168.4.1 255.255.255.0
#
interface GigabitEthernet3/0/0.2
 dot1q termination vid 20
 ip address 192.168.5.1 255.255.255.0
#
return
```

6.9 参考信息

介绍QoS特性的相关参考资料。

文档	描述	备注
RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	-
RFC 2475	An Architecture for Differentiated Services	-
RFC 2597	Assured Forwarding PHB Group	-
RFC 2598	An Expedited Forwarding PHB	-
RFC 2697	A Single Rate Three Color Marker	-
RFC 2698	A Two Rate Three Color Marker	-

7 重标记优先级配置

关于本章

重标记优先级配置介绍了重标记优先级的作用、配置方法和配置示例。

7.1 重标记优先级简介
通过MQC实现重标记优先级。

7.2 应用场景
介绍重标记优先级的应用场景。

7.3 配置重标记优先级
介绍MQC实现重标记优先级详细的配置过程。

7.4 配置举例
通过示例介绍重标记优先级。

7.1 重标记优先级简介

通过MQC实现重标记优先级。

优先级用来标识报文的调度权重或者转发处理优先级别的高低。不同类型的报文根据不同的优先级进行调度或转发。

重标记优先级是指将优先级进行设置，通过提高或降低优先级从而改变报文在网络传输中的状态。例如，对于VLAN报文来说，重标记优先级就是对VLAN报文中的802.1p值进行重新设置，设备根据设置后的802.1p优先级进行调度和转发，改变VLAN报文在二层网络传输中状态。

本章主要介绍通过MQC实现重标记优先级，将符合某类规则的报文进行优先级的重标记，可以将对时延要求高、对服务质量要求高的报文重标记较高的优先级，使这类报文在后续转发中享受较高的调度权重或转发速度，同样的，对时延或服务质量没有特殊要求的报文，可以降低其优先级，为高要求报文提供足够的网络资源。

7.2 应用场景

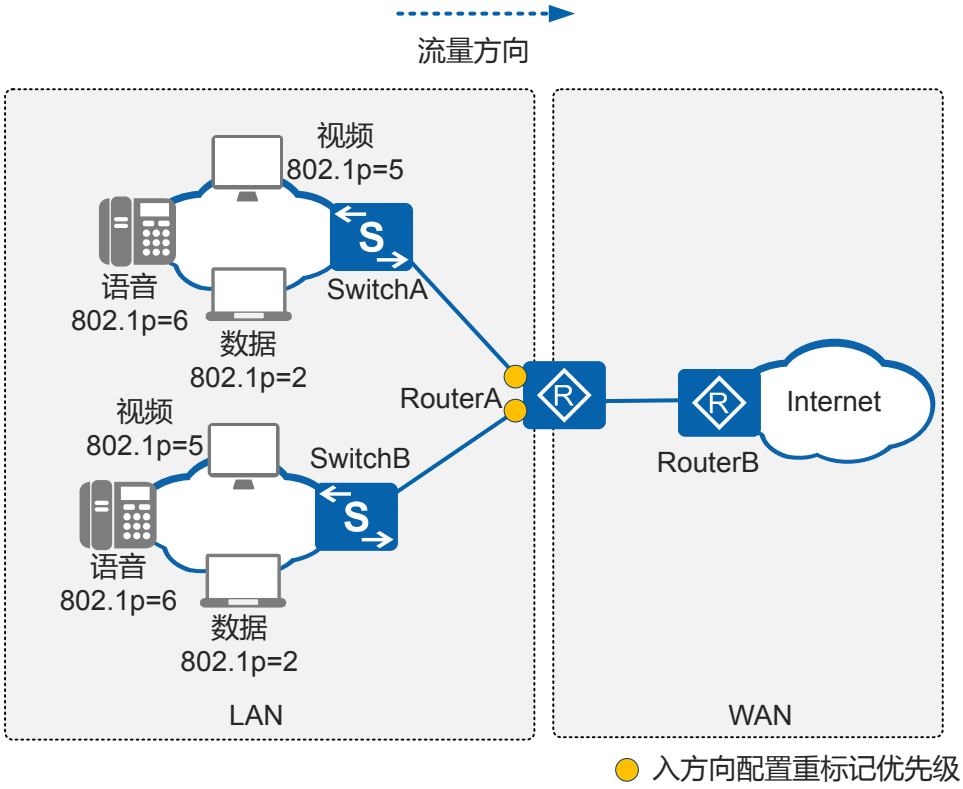
介绍重标记优先级的应用场景。

重标记优先级的应用

重标记优先级可以将对时延要求高、对服务质量要求高的报文重标记较高的优先级，使这类报文在后续转发中享受较高的调度权重或转发速度。

如图7-1所示，不同业务的报文在LAN侧使用802.1p优先级进行标识，当报文到达WAN侧时，用户希望能够根据报文的DSCP优先级针对不同业务提供不同的服务。

图 7-1 重标记优先级应用组网图



业务部署

- 配置流分类，匹配规则为802.1p优先级，从而区分语音、视频、数据报文。
- 配置流行为，重标记三种报文的DSCP优先级，将语音报文的DSCP优先级置为最高，视频报文的DSCP优先级其次，数据报文的DSCP优先级最低。
- 配置流策略，绑定以上流分类和流行为，并应用在RouterA的入方向，实现在三层网络中仍是语音报文的DSCP优先级最高，视频报文的DSCP优先级其次，数据报文的DSCP优先级最低的目的。

7.3 配置重标记优先级

介绍MQC实现重标记优先级详细的配置过程。

背景信息

配置重标记优先级后，设备将对符合流分类规则的报文重标记优先级，使报文根据重标记后的优先级进行调度或转发。

操作步骤

1. 配置流分类
   a. 执行命令**system-view**，进入系统视图。

b. 执行命令**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]，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”，指定该逻辑关系后：

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

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

缺省情况下，流分类中各规则之间的关系为“逻辑或”。

c. 请根据实际情况配置流分类中的匹配规则。

匹配规则	命令
外层VLAN ID	**if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*]
QinQ报文内层VLAN ID	**if-match cvlan-id** *start-vlan-id* [**to** *end-vlan-id*]
VLAN报文802.1p优先级	**if-match 8021p** *8021p-value* &<1-8>
QinQ报文内层VLAN的802.1p优先级	**if-match cvlan-8021p** *8021p-value* &<1-8>
MPLS报文EXP优先级（AR1200&AR2200&AR3200&AR3600系列）	**if-match mpls-exp** *exp-value* &<1-8>
目的MAC地址	**if-match destination-mac** *mac-address* [**mac-address-mask** *mac-address-mask*]
源MAC地址	**if-match source-mac** *mac-address* [**mac-address-mask** *mac-address-mask*]
FR报文中的DLCI信息	**if-match dlci** *start-dlci-number* [**to** *end-dlci-number*]
FR报文中的DE标志位	**if-match fr-de**
以太网帧头中协议类型字段	**if-match l2-protocol** { **arp** | **ip** | **mpls** | **rarp** | *protocol-value* }
所有报文	**if-match any**
IP报文的DSCP优先级	**if-match** [**ipv6**] **dscp** *dscp-value* &<1-8> **说明** 如果流策略中配置了匹配DSCP，则SAE220（WSIC）和SAE550（XSIC）单板不支持**redirect ip-nexthop** *ip-address* **post-nat**动作。

匹配规则	命令
IP报文的IP优先级	**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 [ipv6] dscp**和**if-match ip-precedence**。
报文三层协议类型	**if-match protocol** { **ip** | **ipv6** }
指定QoS group索引的IPSec报文	**if-match qos-group** *qos-group-value*
IPv4报文长度	**if-match packet-length** *min-length* [**to** *max-length*]
ATM报文中的PVC信息	**if-match pvc** *vpi-number/vci-number*
RTP端口号	**if-match rtp start-port** *start-port-number* **end-port** *end-port-number*
TCP报文SYN Flag	**if-match tcp syn-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** }*
入接口	**if-match inbound-interface** *interface-type interface-number*
出接口	**if-match outbound-interface Cellular** *interface-number:channel*
ACL规则	**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。 ● 当使用ACL作为流分类规则匹配源IP地址时，通过在接口下的**qos pre-nat**配置NAT预分类功能，可以将NAT转换前的私网IP地址信息携带到出接口，即可实现基于私网IP地址的分类，从而对来自不同私网IP地址的报文提供差分服务。
ACL6规则	**if-match ipv6 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。 ● 当使用ACL作为流分类规则匹配源IP地址时，通过在接口下的**qos pre-nat**配置NAT预分类功能，可以将NAT转换前的私网IP地址信息携带到出接口，即可实现基于私网IP地址的分类，从而对来自不同私网IP地址的报文提供差分服务。
应用协议	**if-match application** *application-name* [**user-set** *user-set-name*] [**time-range** *time-name*] **说明** 定义基于应用协议的匹配规则前，必须使能SA功能并加载特征库。

匹配规则	命令
SA协议组	**if-match category** *category-name* [**user-set** *user-set-name*] [**time-range** *time-name*] **说明** ● 定义基于应用协议的匹配规则前，必须使能SA功能并加载特征库。
用户组	**if-match user-set** *user-set-name* [**time-range** *time-range-name*]

d. 执行命令**quit**，退出流分类视图。

2. 配置流行为

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

b. 请根据实际需要进行如下配置：

- 执行命令**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VLAN TAG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 mpls-exp** *exp-value*，将符合流分类的报文重新标记EXP优先级。（AR1200系列、AR2200系列、AR3200&AR3600系列）
- 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内部优先级。

  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。

c. 执行命令**quit**，退出流行为视图。

d. 执行命令**quit**，退出系统视图。

3. 配置流策略

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**traffic policy** *policy-name*，创建一个流策略并进入流策略视图，或进入已存在的流策略视图。

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

d. 执行命令**quit**，退出流策略视图。

e. 执行命令**quit**，退出系统视图。

4. 应用流策略

- 在接口下应用流策略

  i. 执行命令**system-view**，进入系统视图。

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

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

- 在安全域间应用流策略

  说明

  仅AR100&AR120&AR150&AR160&AR200系列支持此步骤。

  i. 执行命令**system-view**，进入系统视图。

  ii. 执行命令**firewall interzone** *zone-name1 zone-name2*，创建安全域间并进入安全域间视图。

  缺省情况下，未创建安全域间。

  创建安全域间必须指定两个已存在的安全区域。

  iii. 执行命令**traffic-policy** *policy-name*，在安全域间绑定流策略。

  缺省情况下，安全域间没有绑定流策略。

- 在BD下应用流策略

  说明

  仅在V200R008C30及之后版本，AR100&AR120&AR150&AR160&AR200&AR1200系列和AR2220E支持此步骤。

  i. 执行命令**system-view**，进入系统视图。

  ii. 执行命令**bridge-domain** *bd-id*，创建广播域BD（Bridge Domain）并进入BD视图。

  缺省情况下，没有创建广播域BD。

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

  缺省情况下，BD下没有应用任何流策略。

检查配置结果

- 执行命令**display traffic classifier user-defined** [*classifier-name*]，查看已配置的流分类信息。
- 执行命令**display traffic behavior** { **system-defined** | **user-defined** } [*behavior-name*]，查看已配置的流行为信息。
- 执行命令**display traffic policy user-defined** [*policy-name* [**classifier** *classifier-name*]]，查看流策略的配置信息。
- 执行命令**display traffic-policy applied-record** [*policy-name*]，查看指定流策略的应用记录。

7.4 配置举例

通过示例介绍重标记优先级。

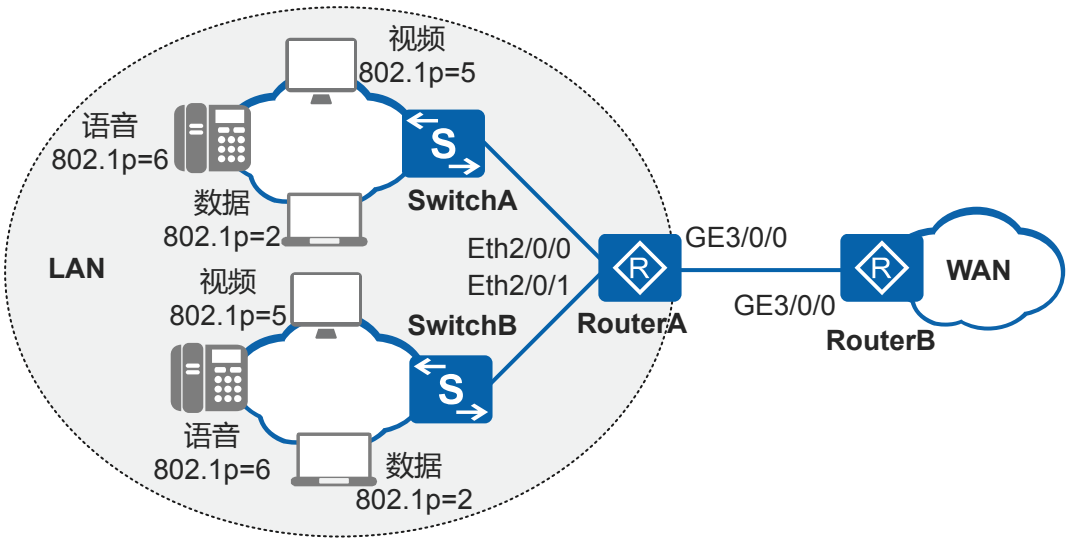
7.4.1 配置重标记优先级示例

组网需求

如图7-2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的接口Eth2/0/0和Eth2/0/1上，并通过RouterA的接口GE3/0/0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，当报文从接口GE3/0/0到达WAN侧时，用户希望能够根据报文的DSCP优先级针对不同业务提供差分服务。

图 7-2 配置重标记的组网图



配置思路

采用将802.1p优先级重标记为DSCP优先级的方式实现差分服务，配置思路如下：

1. 在RouterA上创建VLAN、VLANIF，并配置各接口，实现企业用户能通过RouterA访问WAN侧网络。
2. 在RouterA上配置流分类，实现基于802.1p优先级对报文进行分类。
3. 在RouterA上配置流行为，实现重标记报文的优先级为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Eth2/0/0和Eth2/0/1的入方向上，实现不同业务报文的重标记。

操作步骤

步骤1 创建VLAN并配置各接口

在RouterA上创建VLAN20和VLAN30。

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

配置接口Eth2/0/0和Eth2/0/1的接口类型为Trunk，并将Eth2/0/0加入VLAN20，将Eth2/0/1加入VLAN30。

```
[RouterA] interface ethernet 2/0/0
[RouterA-Ethernet2/0/0] port link-type trunk
[RouterA-Ethernet2/0/0] port trunk allow-pass vlan 20
[RouterA-Ethernet2/0/0] quit
[RouterA] interface ethernet 2/0/1
[RouterA-Ethernet2/0/1] port link-type trunk
[RouterA-Ethernet2/0/1] port trunk allow-pass vlan 30
[RouterA-Ethernet2/0/1] quit
```

说明

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

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

创建VLANIF20、VLANIF30，并为VLANIF20配置IP地址192.168.2.1/24，为VLANIF30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RouterA的接口GE3/0/0的IP地址为192.168.4.1/24。

```
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] ip address 192.168.4.1 24
[RouterA-GigabitEthernet3/0/0] quit
```

配置RouterB的接口GE3/0/0的IP地址为192.168.4.2/24。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface gigabitethernet 3/0/0
[RouterB-GigabitEthernet3/0/0] ip address 192.168.4.2 24
[RouterB-GigabitEthernet3/0/0] quit
```

配置RouterB与LAN侧网络层互通。

```
[RouterB] ip route-static 192.168.2.0 255.255.255.0 192.168.4.1
[RouterB] ip route-static 192.168.3.0 255.255.255.0 192.168.4.1
```

说明

请配置SwitchA对应企业网内用户的缺省网关为192.168.2.1/24。

请配置SwitchB对应企业网内用户的缺省网关为192.168.3.1/24。

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Eth2/0/0和Eth2/0/1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 2/0/0
[RouterA-Ethernet2/0/0] traffic-policy p1 inbound
[RouterA-Ethernet2/0/0] quit
[RouterA] interface ethernet 2/0/1
[RouterA-Ethernet2/0/1] traffic-policy p1 inbound
[RouterA-Ethernet2/0/1] 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 Ethernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 20
 traffic-policy p1 inbound
#
interface Ethernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 30
 traffic-policy p1 inbound
#
interface GigabitEthernet3/0/0
 ip address 192.168.4.1 255.255.255.0
#
return
```

- RouterB的配置文件

```
#
 sysname RouterB
#
interface GigabitEthernet3/0/0
 ip address 192.168.4.2 255.255.255.0
#
ip route-static 192.168.2.0 255.255.255.0 192.168.4.1
ip route-static 192.168.3.0 255.255.255.0 192.168.4.1
#
return
```

8 基于 ACL 的简化流策略配置

关于本章

通过配置基于ACL的简化流策略，对匹配ACL规则的报文进行过滤。

8.1 基于ACL的简化流策略概述
基于ACL的简化流策略是指通过将报文信息与ACL规则进行匹配，为符合相同ACL规则的报文提供相同的QoS服务，实现对不同类型业务的差分服务。

8.2 配置基于ACL的报文过滤
通过配置基于ACL的报文过滤，对匹配ACL规则报文进行禁止/允许动作，进而实现对网络流量的控制。

8.3 维护基于ACL的简化流策略
配置了基于ACL进行报文过滤后，可以查看流量统计信息，分析报文的通过和丢弃情况。

8.4 FAQ
介绍配置基于ACL的简化流策略的FAQ。

8.5 参考信息

8.1 基于 ACL 的简化流策略概述

基于ACL的简化流策略是指通过将报文信息与ACL规则进行匹配，为符合相同ACL规则的报文提供相同的QoS服务，实现对不同类型业务的差分服务。

当用户希望对进入网络的流量进行控制时，可以配置ACL规则根据报文的源IP地址、分片标记、目的IP地址、源端口号、源MAC地址等信息对报文进行匹配，进而配置基于ACL的简化流策略实现对匹配ACL规则的报文过滤。

与流策略相比，基于ACL的简化流策略不需要单独创建流分类、流行为或流策略，配置更为简洁；但是由于仅基于ACL规则对报文进行匹配，因此匹配规则没有流策略丰富。

8.2 配置基于 ACL 的报文过滤

通过配置基于ACL的报文过滤，对匹配ACL规则报文进行禁止/允许动作，进而实现对网络流量的控制。

前置任务

在配置基于ACL的报文过滤之前，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。
- 配置相应的ACL规则。（如果用户需要将ACL规则匹配的报文的IP信息记录日志，可以在**rule**命令行中配置**logging**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**interface** *interface-type interface-number*，进入接口视图。

说明

设备仅支持在WAN侧接口配置基于ACL的报文过滤。

步骤3 执行命令**traffic-filter** { **inbound** | **outbound** } { **acl** | **ipv6 acl** } { *acl-number* | **name** *acl-name* }，配置基于ACL的报文过滤。

说明

在V200R008C30及更低版本，设备的Loopback接口不支持配置该命令。

在V200R008C50及更高版本，设备的Loopback接口支持配置该命令，支持格式为**traffic-filter inbound acl** { *acl-number* | **name** *acl-name* }和**undo traffic-filter inbound**，即设备仅支持在Loopback接口的入方向配置**traffic-filter**命令，并且不支持匹配IPv6 ACL。

步骤4 执行命令**quit**，退出接口视图。

步骤5 （可选）将ACL规则匹配的报文的IP信息记录日志后，执行命令**acl logging** { **timeout** | **update** } { *interval* | **default** }，设置日志刷新以及日志老化的时间间隔。

----结束

检查配置结果

- 执行命令**display traffic-filter applied-record**，查看设备上所有基于ACL进行报文过滤的应用信息。
- 执行命令**display traffic-filter statistics interface** *interface-type interface-number* { **inbound** | **outbound** }或**display traffic-filter statistics interface virtual-template** *vt-number* **virtual-access** *va-number* { **inbound** | **outbound** }，查看指定接口上基于ACL进行报文过滤的流量统计信息。

8.3 维护基于 ACL 的简化流策略

配置了基于ACL进行报文过滤后，可以查看流量统计信息，分析报文的通过和丢弃情况。

8.3.1 查看基于 ACL 的报文过滤的流量统计信息

背景信息

接口上配置基于ACL进行报文过滤后，用户需要了解报文通过和被丢弃的情况时，可以查看其流量统计信息。

操作步骤

- 执行命令**display traffic-filter statistics interface** *interface-type interface-number* { **inbound** | **outbound** } [**verbose rule-base**]或**display traffic-filter statistics interface virtual-template** *vt-number* **virtual-access** *va-number* { **inbound** | **outbound** } [**verbose rule-base**]，查看接口上基于ACL的报文过滤的流量统计信息。

----结束

8.3.2 清除基于 ACL 的报文过滤的流量统计信息

背景信息

当需要对基于ACL的报文过滤的流量统计信息重新进行统计时，可以执行以下命令，清除之前的统计信息。

注意

清除基于ACL的报文过滤的流量统计信息后，以前的统计信息将无法恢复，请于清除之前仔细确认。

操作步骤

- 执行命令**reset traffic-filter statistics interface** *interface-type interface-number* { **inbound** | **outbound** }或**reset traffic-filter statistics interface virtual-template** *vt-*

number **virtual-access** *va-number* { **inbound** | **outbound** }，清除接口上基于ACL的报文过滤的流量统计信息。

----结束

8.3.3 清除基于 ACL 的报文过滤的日志信息

背景信息

当需要清除设备上已经存在的基于ACL的报文过滤的所有日志信息，可以执行以下命令。

操作步骤

- 在用户视图下执行命令**reset acl logging**，清除基于ACL的报文过滤的日志信息。

  说明
  reset acl logging不会清除已打印出的日志。

----结束

8.4 FAQ

介绍配置基于ACL的简化流策略的FAQ。

8.4.1 接口下同时配置 traffic-policy 和 traffic-filter，哪个先生效

从V200R002C00版本开始，新增**traffic-filter**命令。

同时配置时，**traffic-filter**先生效。

8.5 参考信息

介绍QoS特性的相关参考资料。

文档	描述	备注
RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	-
RFC 2475	An Architecture for Differentiated Services	-
RFC 2597	Assured Forwarding PHB Group	-
RFC 2598	An Expedited Forwarding PHB	-
RFC 2697	A Single Rate Three Color Marker	-
RFC 2698	A Two Rate Three Color Marker	-

9 流量统计配置

关于本章

流量统计配置介绍了流量统计的作用、配置方法和配置示例。

9.1 流量统计简介
通过MQC实现流量统计。

9.2 应用场景
介绍流量统计的应用场景。

9.3 配置流量统计
介绍MQC实现流量统计详细的配置过程。

9.4 配置举例
通过示例介绍流量统计。

9.1 流量统计简介

通过MQC实现流量统计。

配置MQC实现流量统计后，设备将对符合流分类规则的报文进行报文数和字节数的统计，可以帮助用户了解应用流策略后流量通过和被丢弃的情况，由此分析和判断流策略的应用是否合理，也有助于进行相关的故障诊断与排查。

只有配置MQC实现流量统计后，才可以通过**display traffic policy statistics**命令查看应用流策略后流量通过和被丢弃的情况。

流量统计与接口统计的区别如表9-1所示。

表 9-1 流量统计与接口统计的区别

统计方式	查询命令	统计范围	说明
流量统计	**display traffic policy statistics**	流策略应用后符合流分类规则的报文	不包括上送CPU报文
接口统计	**display interface**	接口上所有报文	包括上送CPU报文

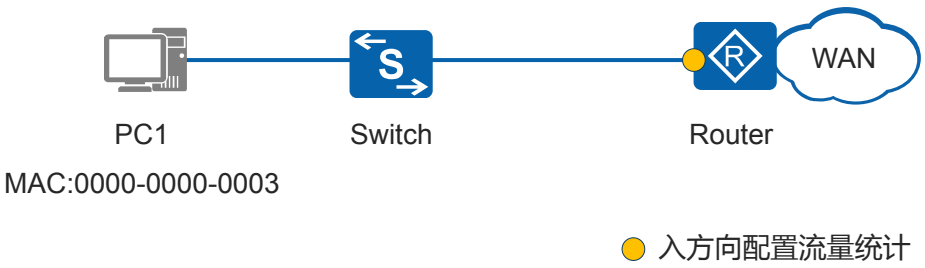
9.2 应用场景

介绍流量统计的应用场景。

流量统计的应用

PC1的MAC地址为0000-0000-0003，它通过交换机连接到WAN侧网络设备上。现希望Router对源MAC为0000-0000-0003的报文进行流量统计。如图9-1所示。

图 9-1 流量统计应用组网图



业务部署

- 配置流分类，匹配规则为源MAC为0000-0000-0003，从而区分PC1的报文。
- 配置流行为，在流行为中配置流量统计。
- 配置流策略，绑定以上流分类和流行为，并应用在Router的入方向，实现对PC1报文的流量统计。

9.3 配置流量统计

介绍MQC实现流量统计详细的配置过程。

背景信息

配置流量统计后，设备将对符合流分类规则的报文进行流量统计，可以帮助用户了解应用流策略后报文通过和被丢弃的情况，由此分析和判断流策略的应用是否合理，也有助于进行相关的故障诊断与排查。

操作步骤

1. 配置流分类
   a. 执行命令**system-view**，进入系统视图。
   b. 执行命令**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]，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”，指定该逻辑关系后：
      - 当流分类中有ACL规则时，报文必须匹配其中一条ACL规则以及所有非ACL规则才属于该类。
      - 当流分类中没有ACL规则时，则报文必须匹配所有非ACL规则才属于该类。

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

      缺省情况下，流分类中各规则之间的关系为“逻辑或”。
   c. 请根据实际情况配置流分类中的匹配规则。

匹配规则	命令
外层VLAN ID	**if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*]
QinQ报文内层VLAN ID	**if-match cvlan-id** *start-vlan-id* [**to** *end-vlan-id*]
VLAN报文802.1p优先级	**if-match 8021p** *8021p-value* &<1-8>
QinQ报文内层VLAN的802.1p优先级	**if-match cvlan-8021p** *8021p-value* &<1-8>
MPLS报文EXP优先级（AR1200&AR2200&AR3200&AR3600系列）	**if-match mpls-exp** *exp-value* &<1-8>
目的MAC地址	**if-match destination-mac** *mac-address* [**mac-address-mask** *mac-address-mask*]
源MAC地址	**if-match source-mac** *mac-address* [**mac-address-mask** *mac-address-mask*]

匹配规则	命令
FR报文中的DLCI信息	**if-match dlci** *start-dlci-number* [**to** *end-dlci-number*]
FR报文中的DE标志位	**if-match fr-de**
以太网帧头中协议类型字段	**if-match l2-protocol** { **arp** | **ip** | **mpls** | **rarp** | *protocol-value* }
所有报文	**if-match any**
IP报文的DSCP优先级	**if-match** [**ipv6**] **dscp** *dscp-value* &<1-8> **说明** 如果流策略中配置了匹配DSCP，则SAE220（WSIC）和SAE550（XSIC）单板不支持**redirect ip-nexthop** *ip-address* **post-nat**动作。
IP报文的IP优先级	**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 [ipv6] dscp**和**if-match ip-precedence**。
报文三层协议类型	**if-match protocol** { **ip** | **ipv6** }
指定QoS group索引的IPSec报文	**if-match qos-group** *qos-group-value*
IPv4报文长度	**if-match packet-length** *min-length* [**to** *max-length*]
ATM报文中的PVC信息	**if-match pvc** *vpi-number*/*vci-number*
RTP端口号	**if-match rtp start-port** *start-port-number* **end-port** *end-port-number*
TCP报文SYN Flag	**if-match tcp syn-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** }*
入接口	**if-match inbound-interface** *interface-type interface-number*
出接口	**if-match outbound-interface Cellular** *interface-number:channel*
ACL规则	**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。 ● 当使用ACL作为流分类规则匹配源IP地址时，通过在接口下的**qos pre-nat**配置NAT预分类功能，可以将NAT转换前的私网IP地址信息携带到出接口，即可实现基于私网IP地址的分类，从而对来自不同私网IP地址的报文提供差分服务。

匹配规则	命令
ACL6规则	**if-match ipv6 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。 ● 当使用ACL作为流分类规则匹配源IP地址时，通过在接口下的**qos pre-nat**配置NAT预分类功能，可以将NAT转换前的私网IP地址信息携带到出接口，即可实现基于私网IP地址的分类，从而对来自不同私网IP地址的报文提供差分服务。
应用协议	**if-match application** *application-name* [**user-set** *user-set-name*] [**time-range** *time-name*] **说明** 定义基于应用协议的匹配规则前，必须使能SA功能并加载特征库。
SA协议组	**if-match category** *category-name* [**user-set** *user-set-name*] [**time-range** *time-name*] **说明** ● 定义基于应用协议的匹配规则前，必须使能SA功能并加载特征库。
用户组	**if-match user-set** *user-set-name* [**time-range** *time-range-name*]

d. 执行命令**quit**，退出流分类视图。

2. 配置流行为
   a. 执行命令**traffic behavior** *behavior-name*，创建一个流行为并进入流行为视图，或进入已存在的流行为视图。
   b. 执行命令**statistic enable**，使能流量统计功能。
      缺省情况下，流行为中未使能流量统计功能。
   c. 执行命令**quit**，退出流行为视图。
   d. 执行命令**quit**，退出系统视图。
3. 配置流策略
   a. 执行命令**system-view**，进入系统视图。
   b. 执行命令**traffic policy** *policy-name*，创建一个流策略并进入流策略视图，或进入已存在的流策略视图。
   c. 执行命令**classifier** *classifier-name* **behavior** *behavior-name*，在流策略中为指定的流分类配置所需流行为，即绑定流分类和流行为。
   d. 执行命令**quit**，退出流策略视图。
   e. 执行命令**quit**，退出系统视图。
4. 应用流策略
   - 在接口下应用流策略
     i. 执行命令**system-view**，进入系统视图。
     ii. 执行命令**interface** *interface-type interface-number* [*.subinterface-number*]，进入接口视图。

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

- 在安全域间应用流策略

  说明

  仅AR100&AR120&AR150&AR160&AR200系列支持此步骤。

  i. 执行命令**system-view**，进入系统视图。

  ii. 执行命令**firewall interzone** *zone-name1 zone-name2*，创建安全域间并进入安全域间视图。

  缺省情况下，未创建安全域间。

  创建安全域间必须指定两个已存在的安全区域。

  iii. 执行命令**traffic-policy** *policy-name*，在安全域间绑定流策略。

  缺省情况下，安全域间没有绑定流策略。

- 在BD下应用流策略

  说明

  仅在V200R008C30及之后版本，AR100&AR120&AR150&AR160&AR200&AR1200系列和AR2220E支持此步骤。

  i. 执行命令**system-view**，进入系统视图。

  ii. 执行命令**bridge-domain** *bd-id*，创建广播域BD（Bridge Domain）并进入BD视图。

  缺省情况下，没有创建广播域BD。

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

  缺省情况下，BD下没有应用任何流策略。

检查配置结果

- 执行命令**display traffic classifier user-defined** [*classifier-name*]，查看已配置的流分类信息。
- 执行命令**display traffic behavior** { **system-defined** | **user-defined** } [*behavior-name*]，查看已配置的流行为信息。
- 执行命令**display traffic policy user-defined** [*policy-name* [**classifier** *classifier-name*]]，查看流策略的配置信息。
- 执行命令**display traffic-policy applied-record** [*policy-name*]，查看指定流策略的应用记录。

9.4 配置举例

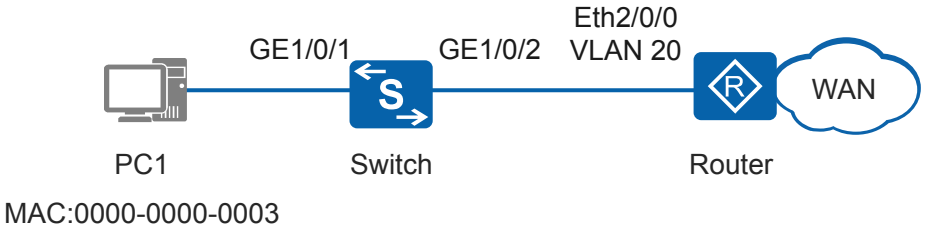
通过示例介绍流量统计。

9.4.1 配置流量统计示例

组网需求

如图9-2所示，PC1的MAC地址为0000-0000-0003，它通过交换机连接到WAN侧网络设备上。现希望Router对源MAC为0000-0000-0003的报文进行流量统计。

图 9-2 配置流量统计组网图



配置思路

采用包含流量统计动作的流策略方式实现流量统计，具体配置思路如下：

1. 配置各接口，实现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，实现基于上述ACL规则对报文进行分类。
4. 配置流行为，实现对满足规则的报文进行流量统计。
5. 配置流策略，绑定上述流分类和流行为，并应用到接口Eth2/0/0的入方向，实现对该接口收到的源MAC为0000-0000-0003的报文进行流量统计。

操作步骤

步骤1 创建VLAN并配置各接口

在Router上创建VLAN20。

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

配置Router上接口Eth2/0/0为Trunk类型接口，并将Eth2/0/0加入VLAN20。

```
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] port link-type trunk
[Router-Ethernet2/0/0] port trunk allow-pass vlan 20
[Router-Ethernet2/0/0] quit
```

在交换机上创建VLAN20，配置接口GE1/0/2为Trunk类型接口，接口GE1/0/1为Access类型接口，并将GE1/0/2加入VLAN20。

```
<Huawei> system-view
[Huawei] sysname Switch
[Switch] vlan 20
[Switch-vlan20] quit
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type access
[Switch-GigabitEthernet1/0/1] port default vlan 20
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk allow-pass vlan 20
[Switch-GigabitEthernet1/0/2] quit
```

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Eth2/0/0。

```
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] traffic-policy p1 inbound
[Router-Ethernet2/0/0] 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 2/0/0 inbound

 Interface: Ethernet2/0/0
 Traffic policy inbound: p1
 Rule number: 1
 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

- 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 Ethernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 20
 traffic-policy p1 inbound
#
return
```

- Switch的配置文件

```
#
 sysname Switch
#
vlan batch 20
#
interface GigabitEthernet1/0/1
 port link-type access
 port default vlan 20
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
return
```

10 带宽管理配置

关于本章

通过配置带宽管理功能，当网络中发生拥塞时，设备可以优先保证关键业务获得带宽，并限制非关键业务的上下行速率。

10.1 带宽管理简介
介绍带宽管理的定义和目的。

10.2 原理描述
介绍了带宽管理涉及的基本概念等。

10.3 应用场景
介绍带宽管理的应用场景。

10.4 配置注意事项
介绍部署带宽管理的注意事项。

10.5 配置带宽管理
介绍带宽管理详细的配置过程。

10.6 配置举例
介绍带宽管理的配置举例。配置举例包括组网需求、配置思路、配置步骤和配置文件等。

10.7 参考信息

10.1 带宽管理简介

介绍带宽管理的定义和目的。

定义

带宽管理是指基于接口入方向、接口出方向、源IP地址、目的IP地址、用户组、时间段和描述信息等，对报文流量进行管理和控制。

目的

带宽管理提供带宽保证和带宽限制的功能，可以提高带宽利用率，避免带宽资源耗尽。

- 带宽保证：保证网络中关键业务所需的带宽，当网络繁忙时，确保此类业务不受影响。
- 带宽限制：限制网络中非关键业务占用的带宽，避免此类业务消耗大量带宽资源，影响其他业务。

在设备上部署带宽管理，可以帮助网络管理员合理分配带宽资源，从而提升网络运营质量。

10.2 原理描述

介绍了带宽管理涉及的基本概念等。

每 IP/每用户组的最大带宽

每IP/每用户组的最大带宽是指基于IP或用户组的报文可获得的最大带宽资源。设备会基于IP或用户组，对符合带宽策略匹配条件的流量进行统计，每一个IP或用户组的流量都不能超过定义的最大带宽。

每 IP/每用户组的保证带宽

每IP/每用户组的保证带宽是指基于IP或用户组的报文可获得的最小带宽资源。设备会从总带宽中划分出一部分带宽为符合条件的IP或用户组流量独享，从而保障即使在网络繁忙状态，指定流量也能够独占保证带宽。

带宽策略

带宽策略决定了对网络中的哪些流量进行带宽管理，以及如何进行带宽管理。

带宽策略是多个带宽策略规则的集合，带宽策略规则由条件和动作组成。

条件指的是设备匹配报文的依据，包括：

- 接口类型和接口编号
- 接口名称
- 入方向
- 出方向

- IP地址
- 用户组
- 时间段

动作指的是设备对报文采取的处理方式，包括：

- 整体限速：对符合条件的用户组下的所有IP进行统一限速。
- 单独限速：对单个IP进行限速。

10.3 应用场景

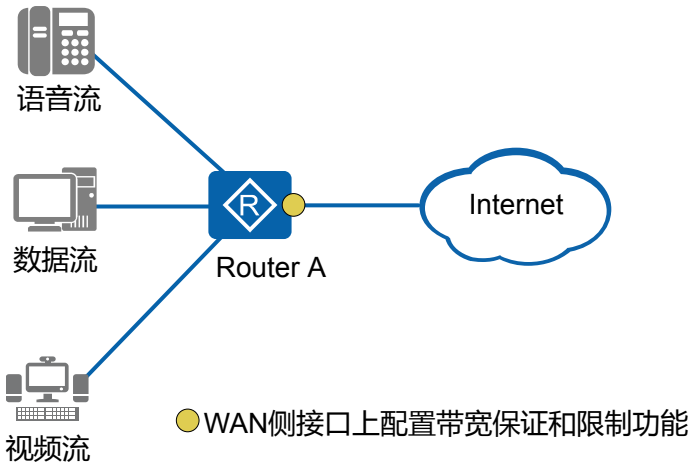
介绍带宽管理的应用场景。

如图10-1所示，企业网内部LAN侧的语音、视频和数据业务共享同一网络的相同带宽，对于带宽资源的使用，通常会面临如下问题：

- 局域网内用户访问Internet时，所需的带宽远大于企业从运营商租用的带宽，存在带宽瓶颈。
- 视频类业务流量消耗了绝大部分的带宽资源，使得语音业务得不到带宽保证。

基于上述情况，可以在RouterA的WAN侧接口上，定义带宽保证或带宽限制规则，用于控制不同业务的数据流量。

图 10-1 带宽管理应用组网图



10.4 配置注意事项

介绍部署带宽管理的注意事项。

涉及网元

无需其他网元配合。

License 支持

带宽管理是设备的基本特性，无需获得License许可即可应用此功能。

版本支持

支持带宽管理的最低软件版本如表10-1所示。

表 10-1 产品形态和最低软件版本支持情况

系列	最低版本支持情况
AR100系列	V200R008C30
AR120系列	V200R007C00
AR160系列 **说明** 仅AR161、AR161W、AR161G-L、AR161G-Lc、AR161EW、AR161EW-M1、AR169EW、AR169CVW、AR169CVW-4B4S、AR169EGW-L、AR161G-U、AR169、AR169G-L、AR169-P-M9、AR169W-P-M9和AR169RW-P-M9支持。	V200R007C00

10.5 配置带宽管理

介绍带宽管理详细的配置过程。

背景信息

配置带宽管理后，设备将对符合条件的报文进行带宽控制，从而实现对网络流量的管理。

操作步骤

- 配置带宽保证。
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**web**，进入Web视图。
  c. （可选）执行命令**user-set** *user-set-name*，创建一个Web用户组并进入Web用户组视图，或直接进入一个已存在的Web用户组视图。
     缺省情况下，设备中存在一个名为VIP，一个名为Default的Web用户组。
  d. （可选）执行命令**user-ip from** *ip_addr1* **to** *ip_addr2* [**description** *description*]，配置Web用户组中用户IP段。
     缺省情况下，未配置Web用户组中的用户IP段。
  e. 执行命令**bandguarantee interface** { *interface-type interface-number* | *interface-name* } **type** { **ip** *ip-address* | **user-set** *user-set-name* } **cir** *cir-value* [**time-range** *time-range-name*] [**description** *desctiption*]，配置用户带宽保证功能。
     缺省情况下，没有配置用户带宽保证功能。

f. 执行命令**quit**，退出web视图。

g. 执行命令**quit**，退出系统视图。

- 配置带宽限制。

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**web**，进入web视图。

c. （可选）执行命令**user-set** *user-set-name*，创建一个Web用户组并进入Web用户组视图，或直接进入一个已存在的Web用户组视图。

缺省情况下，设备中存在一个名为VIP，一个名为Default的Web用户组。

d. （可选）执行命令**user-ip from** *ip_addr1* **to** *ip_addr2* [**description** *description*]，配置Web用户组中用户IP段。

缺省情况下，未配置Web用户组中的用户IP段。

e. 执行命令**bandlimit interface** { *interface-type interface-number* | *interface-name* } **type** { **ip** *ip-address* { { **inbound cir** *in-cir-value* | **outbound cir** *out-cir-value* } * } | **user-set** *user-set-name* { { **inbound cir** *in-cir-value* | **outbound cir** *out-cir-value* } * [**share**] } } [**time-range** *time-range-name*] [**description** *desctiption*]，配置用户带宽限制功能。

缺省情况下，没有配置用户带宽限制功能。

f. 执行命令**quit**，退出web视图。

g. 执行命令**quit**，退出系统视图。

后续任务

- 执行命令**disable bandguarantee interface** { *interface-type interface-number* | *interface-name* } **type** { **ip** *ip-address* | **user-set** *user-set-name* } **cir** *cir-value* [**time-range** *time-range-name*] [**description** *desctiption*]，去使能配置的用户带宽保证功能。
- 执行命令**disable bandlimit interface** { *interface-type interface-number* | *interface-name* } **type** { **ip** *ip-address* [{ **inbound cir** *in-cir-value* | **outbound cir** *out-cir-value* } *] | **user-set** *user-set-name* [{ **inbound cir** *in-cir-value* | **outbound cir** *out-cir-value* } * [**share**]] } [**time-range** *time-range-name*] [**description** *desctiption*]，去使能配置的用户带宽限制功能。

检查配置结果

执行命令**display current-configuration**，查看设备当前生效的配置参数。

10.6 配置举例

介绍带宽管理的配置举例。配置举例包括组网需求、配置思路、配置步骤和配置文件等。

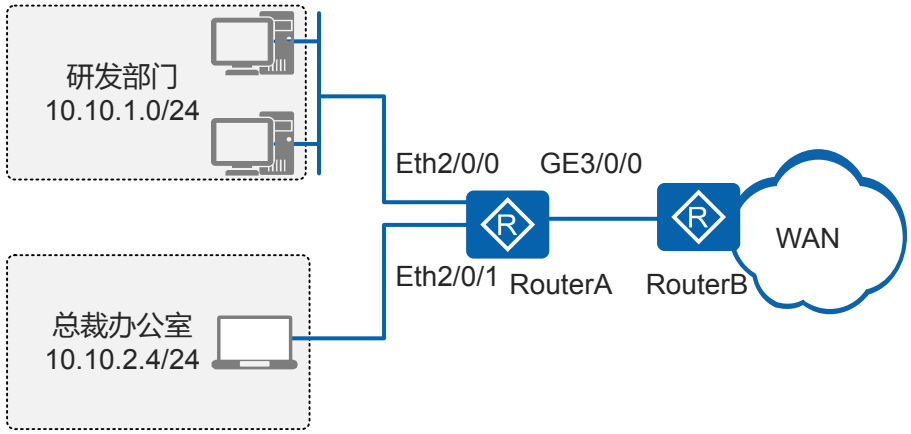
10.6.1 配置带宽管理示例

组网需求

如图10-2所示，公司企业网通过RouterA实现各部门之间的互连，通过RouterA的GE3/0/0接口连接到WAN侧网络。现要求正确配置带宽管理功能，实现如下需求：

- 限制研发部门在工作时间（周一至周五8：00至17:30）与Internet之间的报文下行速率不超过256kbit/s。
- 优先发送总裁办公室的报文，确保在拥塞发生时，总裁办公室获取的最小带宽为2048kbit/s。

图 10-2 配置带宽管理组网图



配置思路

采用如下的思路配置带宽管理：

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. 配置时间段。
3. 在RouterA的GE3/0/0接口上，为企业内各部门设置不同的带宽。

操作步骤

步骤1 创建VLAN和VLANIF，并配置各接口

在RouterA上创建VLAN10和VLAN20。

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

配置RouterA的Eth2/0/0、Eth2/0/1接口类型为Access，并将Eth2/0/0、Eth2/0/1分别加入VLAN10和VLAN20。

```
[RouterA] interface ethernet 2/0/0
[RouterA-Ethernet2/0/0] port link-type access
[RouterA-Ethernet2/0/0]  port default vlan 10
[RouterA-Ethernet2/0/0] quit
[RouterA] interface ethernet 2/0/1
[RouterA-Ethernet2/0/1] port link-type access
[RouterA-Ethernet2/0/1]  port default vlan 20
[RouterA-Ethernet2/0/1] quit
```

创建VLANIF10和VLANIF20，并为VLANIF10配置IP地址10.10.1.1/24，为VLANIF20配置IP地址10.10.2.1/24。

```
[RouterA] interface vlanif 10
[RouterA-Vlanif10] ip address 10.10.1.1 24
[RouterA-Vlanif10] quit
[RouterA] interface vlanif 20
[RouterA-Vlanif20] ip address 10.10.2.1 24
[RouterA-Vlanif20] quit
```

配置RouterA的接口GE3/0/0的IP地址为1.1.1.1/24。

```
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] ip address 1.1.1.1 24
[RouterA-GigabitEthernet3/0/0] quit
```

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 配置时间段

配置8:00至17:30的周期时间段。

```
[RouterA] time-range worktime 8:00 to 17:30 working-day
```

步骤3 在RouterA的GE3/0/0接口上，为企业内各部门设置不同的带宽。

在RouterA的GE3/0/0接口上，配置工作时间段研发部门的报文下行速率不超过256kbit/s。

```
[RouterA] web
[RouterA-web] user-set vd
[RouterA-web-user-set-vd] user-ip from 10.10.1.2 to 10.10.1.254
[RouterA-web-user-set-vd] quit
[RouterA-web] bandlimit interface gigabitethernet 3/0/0 type user-set vd inbound cir 256 time-range worktime
[RouterA-web] quit
```

在RouterA的GE3/0/0接口上，配置总裁办公室获取的最小带宽不低于2048kbit/s。

```
[RouterA] web
[RouterA-web] bandguarantee interface gigabitethernet 3/0/0 type ip 10.10.2.4 cir 2048
[RouterA-web] quit
```

步骤4 验证配置结果

查看RouterA上的带宽管理配置信息，相关信息如下。

```
<RouterA> display current-configuration
#
traffic classifier Class10.10.2.4 operator or
 if-match acl Acl10.10.2.4
#
traffic behavior Behavior10.10.2.4
 queue af bandwidth 2048
 statistic enable
#
traffic policy GigabitEthernet3/0/0
 classifier Class10.10.2.4 behavior Behavior10.10.2.4
#
interface GigabitEthernet3/0/0
 qos car inbound destination-ip-address range 10.10.1.2 to 10.10.1.254 cir 256 c
bs 48128 pbs 80128 green pass yellow pass red discard
 traffic-policy GigabitEthernet3/0/0 outbound
#
return
```

----结束

配置文件

- RouterA的配置文件

```
#
 sysname RouterA
#
 time-range worktime 08:00 to 17:30 working-day
#
vlan batch 10 20
#
web
 user-set vd
  user-ip from 10.10.1.2 to 10.10.1.254
 bandlimit interface GigabitEthernet3/0/0 type user-set vd inbound cir 256 time-
range worktime
 bandguarantee interface GigabitEthernet3/0/0 type ip 10.10.2.4 cir 2048
#
traffic classifier Class10.10.2.4 operator or
 if-match acl Acl10.10.2.4
#
traffic behavior Behavior10.10.2.4
 queue af bandwidth 2048
 statistic enable
#
traffic policy GigabitEthernet3/0/0
 classifier Class10.10.2.4 behavior Behavior10.10.2.4
#
interface Vlanif10
 ip address 10.10.1.1 255.255.255.0
#
interface Vlanif20
 ip address 10.10.2.1 255.255.255.0
#
interface Ethernet0/0/1
 port link-type access
 port default vlan 10
#
interface Ethernet0/0/2
 port link-type access
 port default vlan 20
#
interface GigabitEthernet3/0/0
 ip address 1.1.1.1 255.255.255.0
 qos car inbound destination-ip-address range 10.10.1.2 to 10.10.1.254 cir 256 c
bs 48128 pbs 80128 green pass yellow pass red discard
 traffic-policy GigabitEthernet3/0/0 outbound
#
return
```

10.7 参考信息

介绍QoS特性的相关参考资料。

文档	描述	备注
RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	-
RFC 2475	An Architecture for Differentiated Services	-
RFC 2597	Assured Forwarding PHB Group	-
RFC 2598	An Expedited Forwarding PHB	-
RFC 2697	A Single Rate Three Color Marker	-

文档	描述	备注
RFC 2698	A Two Rate Three Color Marker	-

11 SAC 配置

关于本章

SAC配置介绍SAC等基本概念并介绍SAC的配置方法、配置示例。

11.1 SAC 简介

定义

业务感知SA（Service Awareness）是一个智能的应用协议识别与分类引擎，智能应用控制SAC（Smart Application Control）是指利用业务感知技术，对报文中的第4～7层内容（如HTTP、RTP）进行检测和识别，根据分类结果实施精细化QoS策略控制。

目的

随着网络技术和多媒体技术的快速发展，网络应用越来越丰富，使得带宽资源日趋紧张，其中影响比较突出的是P2P技术。P2P应用类型也已从文件共享扩展到语音、视频等应用领域，P2P网络的用户规模和流量均呈爆发式增长，甚至很多P2P应用往往是对网络资源进行“恶意”占用，导致网络出现不同程度的拥塞。这些流量与关键应用混杂在一起，导致非关键业务占用大量流量，核心业务丢包，时延抖动不可控，服务质量无法保障。用户急需对这些“非法”的网络应用进行控制，于是产生了业务感知技术。

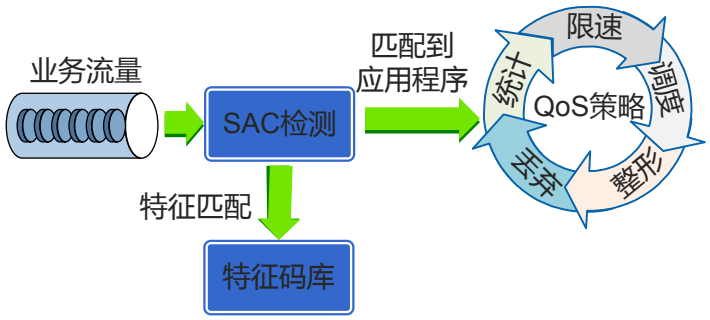
传统流量分类技术只能检测IP报文的4层以下的内容，包括源地址、目的地址、源端口、目的端口以及业务类型等，而无法分析出报文的应用。 业务感知技术在分析报文头的基础上，增加了对应用层的分析，是一种基于应用层的流量检测和控制技术。通过对各类应用进行智能分类，识别关键业务，保证其带宽，对非关键业务流量进行限制，从而保证关键业务平稳、高效运转。

11.2 原理描述

SAC 识别应用程序

特征识别技术是业务感知技术的最基本技术。不同的应用程序通常会采用不同的协议，而不同的应用协议具有各自的特征，这些特征可能是特定的端口、特定的字符串或者特定的比特序列，能标识该协议的特征称为特征码。特征识别技术，即通过匹配数据报文中的特征码来确定应用。协议的特征不仅在单个报文中体现，某些协议报文的特征是分布在多个报文中的，需要对多个报文进行采集分析，才能够识别出协议类型。系统对流经设备的业务流进行分析，将分析结果和加载到设备上的特征库进行对比，通过匹配数据报文中的特征码来识别出应用程序，根据识别结果实施精细化QoS策略控制。SAC工作机制如图11-1所示。

图 11-1 SAC 工作机制



设备都是通过应用协议的特征码识别应用协议报文，但是应用软件会不断升级和更新，其特征码也会发生变化，导致原有特征码无法正确或精确匹配应用协议，特征码需要及时更新，如果在产品软件包中固化特征码，就要更换新的软件版本，对业务影响较大。华为公司设备通过特征库文件和系统软件分离，可以随时对特征码文件进行加载和升级，而不影响其他业务的正常运行。

华为公司通过分析各种常见应用形成了特征库文件，特征库文件以预定义方式加载到设备上。加载SAC特征库文件之后，系统会自动生成45个应用组，其中包括Instant_Messaging应用组，Instant_Messaging应用组包括当前最常见的即时通信软件：QQ_IM、MSN_IM、ICQ_IM、YahooMsg_IM、SinaUC_IM、Fetion_IM、AliTalk_IM、DoShow_IM、XiaoNeiTong、Skype_IM、Lava_Lava_IM和GoogleTalk_IM。预定义的特征库文件只能以升级的方式进行更新，不可以手动修改。预定义的特征库所包含的常见应用组及其组内的应用协议如表11-1所示。

表 11-1 设备预定义的特征库所包含的常见应用组及其组内常见应用协议

应用组	应用协议
FileShare_P2P	BT
	Thunder
	eDonkey_eMule
	Fasttrack
	DirectConnect
	KuGoo
	PPGou
	POCO
	BaiBao
	Maze
	Vagaa
	QQDownLoad
	Filetopia
	Soulseek
	KooWo
	Foxy
	SpeedUpper

SAC 流量统计

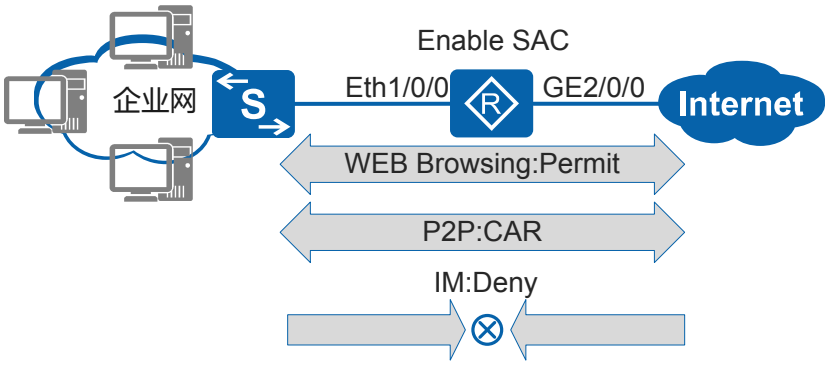
在接口使能SAC流量统计功能时，设备会自动识别并对不同应用的流量进行统计。网络管理员可以及时掌握网络流量情况，从而优化网络部署，合理分配带宽。

11.3 应用场景

如图11-2所示，企业网用Router作为出口网关接入到广域网，为了保证网络质量，并规范员工的上网行为，可以通过使用业务感知技术识别网络中的各种应用程序，并对识别到的各种类型的应用协议加以控制。例如：

- 对于一般的网络浏览行为予以放行，保证内部用户能够访问网络，正常办公。
- 对于QQ等Instant_Messaging类型应用程序进行阻断，限制企业员工从事与工作无关的事务，规范用户上网行为。
- 对于BT、eDonkey_eMule等FileShare_P2P报文则限制其带宽，保证网络质量。

图 11-2 业务感知应用场景



11.4 配置注意事项

介绍配置SAC的注意事项。

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，请根据设备款型联系华为办事处申请并购买如下License：

- 对于AR150&AR160&AR200系列设备：AR150&160&200 安全业务增值包
- 对于AR1200系列设备：AR1200 安全业务增值包
- 对于AR2200系列设备：AR2200 安全业务增值包
- 对于AR3200系列设备：AR3200 安全业务增值包
- 对于AR3600系列设备：AR3600 安全业务增值包

11.5 配置 SAC

前置任务

在配置SAC之前，需要完成以下任务：

- 配置相关接口的IP地址和路由协议，保证路由互通。

配置流程

11.5.1 开启深度安全防御功能并加载 SA 特征库

背景信息

如果需要使用SAC功能，除购买对应License外，同时还需要通过执行**engine enable**命令开启深度安全防御功能。

开启深度安全防御功能后，若首次使用SAC功能，还需通过**update restore sdb-default**命令，手动加载SA特征库文件。

设备内存剩余空间需大于特征库文件大小，才能正常加载特征库文件。

操作步骤

步骤1 执行命令**engine enable**，开启深度安全防御功能。

说明

执行**engine enable**命令后，可通过**display sa information**命令，查看SA状态，若SA状态为enabled，表明深度安全防御功能已开启。

步骤2 执行命令**update restore sdb-default**，将特征库恢复到出厂默认版本。

----结束

11.5.2 （可选）配置 SA 检测参数

背景信息

特征识别技术，通过匹配数据报文中的特征码来确定应用类型。协议的特征不仅在单个报文中体现，某些协议报文的特征是分布在多个报文中的，因此需要对多个报文进行采集、分析，只有将报文的检测参数设置在合理范围内，才能正确识别出协议类型。推荐使用默认缺省值。

操作步骤

步骤1 执行命令**sa**，进入SA视图。

步骤2 执行命令**detect max-packets** *max-packets*，设置SA模块中会话的最大包检测个数。

步骤3 执行命令**detect max-bytes** *max-bytes*，设置SA模块中会话的最大检测字节数。

步骤4 执行命令**port-identification packet-number-threshold** *packets*，设置SA模块启用端口识别的报文阈值。

步骤5 执行命令**detect uni-direction**，设置SA模块开启单向检测模式。

----结束

11.5.3 配置 SAC 流分类规则

背景信息

SAC流分类是指根据一定的规则，把具有某些共同特征的应用层报文划分为同一类，可以针对不同类型的业务流进行差异化服务。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 配置SAC流分类规则。

- 如果需要匹配单个应用协议如BT，请进行如下配置：
  a. 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。
  b. 执行命令**if-match application** *application-name* [**user-set** *user-set-name*] [**time-range** *time-name*]，定义基于应用协议的匹配规则。
- 如果需要匹配单个应用组，请进行如下配置：
  a. 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。
  b. 执行命令**if-match category** *category-name* [**user-set** *user-set-name*] [**time-range** *time-name*]，定义基于SAC应用组的匹配规则。

----结束

11.5.4 配置流行为

背景信息

SAC流分类根据一定的规则，把具有某些共同特征的应用层报文划分为同一类，通过配置流行为，可以针对不同类型的业务流采取不同的动作，进行差异化服务。

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

步骤3 请根据实际情况定义流行为中的动作，只要各动作不冲突，都可以在同一流行为中配置。

动作	命令
配置报文过滤	**deny | permit**
配置报文所属的QoS组	**remark qos-group** *qos-group-value*

动作	命令
配置MQC实现重标记优先级	**remark 8021p** *8021p-value* **remark cvlan-8021p** *8021p-value* **remark dscp** { *dscp-name* | *dscp-value* } **remark mpls-exp** *exp-value*（AR1200&AR2200&AR3200&AR3600系列） **remark fr-de** *fr-de-value* **remark local-precedence** *local-precedence-value* **说明** 如果在流行为中配置了**remark 8021p**、**remark mpls-exp**、**remark dscp**，未配置**remark local-precedence**，报文中的本地优先级会被标记为0。
配置MQC实现流量监管	**car cir** { *cir-value* | **pct** *cir-percentage* } [**pir** { *pir-value* | **pct** *pir-percentage* }] [**cbs** *cbs-value* **pbs** *pbs-value*] [**share**] [**mode** { **color-blind** | **color-aware** }] [**green** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] [**yellow** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] [**red** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] **说明** AR100&AR120&AR150&AR160&AR200系列不支持**remark-mpls-exp** *exp-value*参数。
配置MQC实现流量整形	**gts cir** { *cir-value* [**cbs** *cbs-value*] | **pct** *pct-value* } [**queue-length** *queue-length*]
配置MQC实现自适应流量整形	**gts adaptation-profile** *adaptation-profile-name*
配置MQC实现拥塞管理	**queue af bandwidth** { *bandwidth* | [**remaining**] **pct** *percentage* } **queue ef bandwidth** { *bandwidth* [**cbs** *cbs-value*] | **pct** *percentage* [**cbs** *cbs-value*] } **queue llq bandwidth** { *bandwidth* [**cbs** *cbs-value*] | **pct** *percentage* [**cbs** *cbs-value*] } **queue wfq** [**queue-number** *total-queue-number*] **queue-length** { **bytes** *bytes-value* | **packets** *packets-value* }*
配置MQC实现拥塞避免	**drop-profile** *drop-profile-name*
配置MQC实现Netstream统计采样	**ip netstream sampler** { **fix-packets** *packet-interval* | **fix-time** *time-interval* | **random-packets** *packet-interval* | **random-time** *time-interval* } { **multicast** | **rpf-failure** | **unicast** }* **说明** ● IPv6和MPLS报文不支持配置Netstream统计采样功能，因此对应的流分类规则不能包含IPv6或MPLS关键字。 ● V200R008C50及以后版本，二层VE接口不支持该功能。

动作	命令
配置单播策略路由	**redirect ip-nexthop** *ip-address* [**track** { **nqa** *admin-name test-name* | **ip-route** *ip-address* { *mask* | *mask-length* } }] [**post-nat**] [**discard**] **说明** 如果流策略中配置了匹配DSCP，则SAE220（WSIC）和SAE550（XSIC）单板不支持**redirect ip-nexthop** *ip-address* **post-nat**动作。 **redirect ipv6-nexthop** *ipv6-address* [**track** { **nqa** *nqa-admin nqa-name* | **ipv6-route** *ipv6﹣address mask-length* }] [**discard**] **redirect interface** *interface-type interface-number* [**track** { **nqa** *admin-name test-name* | **ip-route** *ip-address* { *mask* | *mask-length* } | **ipv6-route** *ipv6-address mask-length* }] [**discard**] **redirect vpn-instance** *vpn-instance-name* **说明** V200R008C50及以后版本，二层VE接口不支持该功能。
配置绑定子策略	**traffic-policy** *policy-name*
配置流量统计	**statistic enable**
配置MQC实现URL过滤	**url-filter-profile** *profile-name*

步骤4 执行命令**quit**，退出流行为视图。

----结束

11.5.5 配置流策略

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**traffic policy** *policy-name*，创建一个流策略并进入流策略视图，或进入已存在的流策略视图。

步骤3 执行命令**classifier** *classifier-name* **behavior** *behavior-name*，在流策略中为指定的流分类配置所需流行为，即绑定流分类和流行为。

----结束

11.5.6 应用 SAC 策略

背景信息

在WAN侧接口应用流策略，可以对经过接口的报文进行分析，对符合规则的应用层协议采用相应的动作，实现对业务的精细化管理。

说明

配置SAC功能的流策略只能在三层接口应用。

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**traffic-policy** *policy-name* { **inbound** | **outbound** }，在接口的出/入方向应用流策略。

----结束

11.5.7 检查配置结果

前提条件

已经完成SAC的配置。

操作步骤

步骤1 执行命令**display sa information**，查看设备的SA相关配置信息。

步骤2 执行命令**display sa category** [*category-name*]，查看SA协议组的配置信息。

步骤3 执行命令**display sa application-list**，查看当前设备支持的SA协议列表。

步骤4 执行命令**display application**，查看系统中的应用的相关信息。

步骤5 执行命令**display application name aging-time**，查看应用识别关联表的老化时间。

----结束

11.6 维护 SAC

11.6.1 升级 SAC 特征库

背景信息

SAC特征库的升级方式有：

- 在线升级
  - 当设备能访问安全中心平台时，可以配置通过安全中心平台进行在线升级。
  - 当设备无法访问安全中心平台时，可以配置通过内网升级服务器进行在线升级。
    i. 请确保内网升级服务器可以正常访问安全中心平台。
    ii. 请确保设备和内网升级服务器之间的路由互通。
- 本地升级

  当设备无法访问安全中心平台时，用户也可以在能够访问安全中心平台的PC上下载升级包，通过FTP或TFTP等方式将SAC特征库文件上传到设备上进行本地升级。

说明

SAC特征库升级以后，新的特征库可能会对应用组的分类进行调整，分类下的应用协议也会有所调整。此时如果设备上存在基于应用组的配置，可能会导致相关业务失效。此时用户可以通过**display sa category**命令查看新的特征库的分组情况，通过**display application**命令查询系统中应用的相关信息，并对配置进行调整。

操作步骤

- 在线升级
  a. 执行命令**system-view**，进入系统视图。
  b. （可选）执行命令**update server** { **domain** *domain-name* | **ip** *ip-address* } [**port** *port-number*]，配置升级服务器的IP地址或者域名。
     缺省情况下，升级服务器的域名为sec.huawei.com，端口号默认为80。
  c. （可选）通过代理服务器访问升级服务器。
     i. 执行命令**update proxy enable**，用来开启特征库代理升级功能。
        缺省情况下，设备没有开启特征库代理升级功能。
     ii. 执行命令**update proxy** { **domain** *domain-name* | **ip** *ip-address* } [**port** *port-number*] [**user** *user-name* [**password** *password*]]，用来配置代理服务器的IP地址或者域名。
  d. 确定在线升级方式
     - 通过安全中心平台进行在线升级
       为保证设备能访问安全中心平台，需要配置动态域名解析功能。
       1) 执行命令**dns resolve**，启用DNS服务器的域名解析功能。
       2) 执行命令**dns server** *ip-address*，配置DNS服务器的IP地址。
  e. 选择定时升级还是立即升级
     一般用户可选择定时升级。设备的定时升级时间尚未达到时，用户也可以执行立即升级。
     - 定时升级
       1) 执行命令**update schedule sa-sdb enable**，开启SAC特征库的定时升级功能。
          缺省情况下，已开启SAC特征库定时升级功能。
       2) 执行命令**update schedule** [{ **daily** | **weekly** { **Mon** | **Tue** | **Wed** | **Thu** | **Fri** | **Sat** | **Sun** } } *time*]，用来配置SAC特征库定时在线下载时间。
          如果未配置定时下载时间，则缺省在22：00～08：00之间随机选择一个时间作为每天进行定时升级的时间。
          *time*建议设置为一天中设备流量最小的时间，例如凌晨6点前后。
       3) 配置SAC特征库安装方式
          SAC特征库下载后，还需要在设备上进行安装才生效。用户可以选择是否使能安装确认功能，即定时升级的SAC特征库是否需要经过用户确认后再安装。
          SAC特征库安装时涉及新旧SAC特征库的切换，用户可以选择影响较小时启用安装确认功能。
          - 用户确认后进行安装

1) 执行命令**update confirm sa-sdb enable**，用来使能安装确认功能，即定时下载的SAC特征库需要经过用户确认后再安装。

缺省情况下，所有的自动安装确认功能关闭，即设备定时下载的升级文件自动进行安装。

2) 执行命令**update apply sa-sdb**，安装下载的SAC特征库。

- 用户无需确认即直接安装

执行命令**undo update confirm sa-sdb enable**，用来去使能安装确认功能，即定时下载的SAC特征库进行自动安装，不需要经过用户确认。

- 立即升级

1) 执行命令**update online sa-sdb**，用来立即下载SAC特征库。
2) 执行命令**update apply sa-sdb**，用来安装下载的SAC特征库。

- 终止升级

在用户开始升级后，发现升级过程占用了较大网络资源，可以终止升级。

说明

只有在下载阶段才可以终止升级。

a. 执行命令**system-view**，进入系统视图。
b. 执行命令**update abort**，用来终止升级。

- 回退版本

如果升级后的特征库出现问题或不符合用户预期，用户可使用该命令回退到上一个版本。

说明

进行版本回退前，建议先使用**display version sa-sdb**命令查看可回退版本信息，再决定是否要进行版本回退。如果不存在可回退版本，版本回退将失败，设备中仍然是回退前的版本。

a. 执行命令**system-view**，进入系统视图。
b. 执行命令**update rollback sa-sdb**，用来回退SAC特征库到上一个版本。

- 本地升级

a. 执行命令**system-view**，进入系统视图。
b. 执行命令**update local sa-sdb file** *filename*，用户进行本地升级SAC特征库。

说明

本地升级不支持**终止升级**。

- 恢复出厂默认版本

说明

特征库恢复到出厂默认版本后，设备上其他所有SAC特征库均被删除，

a. 执行命令**system-view**，进入系统视图。
b. 执行命令**update restore sdb-default sa-sdb**，将特征库恢复到出厂默认版本。

----结束

升级结果验证

- 执行命令**display engine information**，显示引擎的运行状态和特征库的版本信息。

- 执行命令**display version sa-sdb**，查看升级后SAC特征库的版本信息。
- 执行命令**display update status**，查看升级的状态。
- 执行命令**display update configuration**，查看升级配置信息。

11.6.2 恢复出厂默认版本

背景信息

当特征库升级出现异常时，可将特征库恢复到出厂默认版本后再进行升级操作。

注意

特征库恢复到出厂默认版本后，Router上其他所有特征库版本均被删除，因此请慎用这个功能。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**update restore sdb-default sa-sdb**，恢复特征库为出厂默认版本。

----结束

11.6.3 查看应用协议报文统计信息

前提条件

使能SA功能并加载特征库。

背景信息

当用户在接口上使能了SA统计功能时，可以查看接口上通过的基于不同SA应用协议的报文统计信息，也可以查看设备上报文字节数最多的多种应用协议的报文统计信息。通过了解应用协议报文的信息，及时掌握网络使用情况。

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**sa application-statistic enable**，使能SA统计功能。

步骤4 执行命令**display sa application-statistic** { **application** *application-name* | **top-n** *number* | **all** } **interface** { *interface-type interface-number* | **virtual-template** *vt-number* **virtual-access** *va-number* } [**inbound** | **outbound**]，查看应用协议的报文统计信息。

注意

执行**reset session all**命令删除所有流表信息后，需要同步执行**reset engine session table**命令清除引擎的会话信息，才能继续对应用协议的报文信息进行统计。

SA功能对已建立链接的协议不能识别，需要断开已有链接，重新建立链接，SA功能方能生效。

----结束

11.6.4 清除应用协议报文统计信息

背景信息

为了能够清楚地查看某一时间段内设备正常通信的报文，可以执行下面的命令先清空之前的报文统计数。

注意

清除应用协议报文统计信息后，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 sa application-statistic** { **application** *application-name* | **all** } **interface** { *interface-type interface-number* | **virtual-template** *vt-number* **virtual-access** *va-number* }，清除应用层协议统计信息。

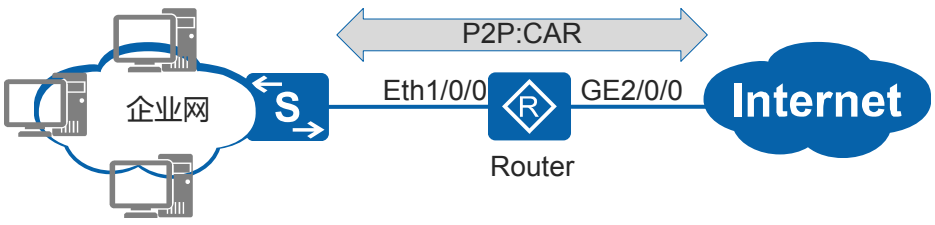
11.7 配置举例

11.7.1 配置 FileShare_P2P 流量限速示例

组网需求

如图11-3所示，某企业通过Router作为网关设备连接到外网，为了保证网络质量，避免浪费带宽，保证其他业务正常运行，设备检测到BT、eDonkey_eMule等FileShare_P2P报文，则将FileShare_P2P报文速度限制在4Mbit/s以内。

图 11-3 配置 FileShare_P2P 流量限速示例典型组网图



配置思路

采用如下思路配置SAC：

1. 开启深度安全防御功能，并加载特征库文件。
2. 配置流分类，匹配FileShare_P2P协议组。
3. 配置流行为，将匹配到的FileShare_P2P速率限制在4Mbit/s以内。
4. 配置流策略，将流分类和流行为绑定。
5. 在WAN侧接口入方向应用流策略。

操作步骤

步骤1 开启深度安全防御功能，并加载特征库文件

```
<Huawei> system-view
[Huawei] sysname Router
[Router] engine enable
```

步骤2 配置流分类，识别FileShare_P2报文

```
[Router] traffic classifier p2p
[Router-classifier-p2p] if-match category FileShare_P2P
[Router-classifier-p2p] quit
```

步骤3 配置流行为，对识别出的FileShare_P2P报文进行限速

```
[Router] traffic behavior p2p
[Router-behavior-p2p] car cir 4096
[Router-behavior-p2p] quit
```

步骤4 配置流策略，将流分类和流行为绑定

```
[Router] traffic policy p2p
[Router-trafficpolicy-p2p] classifier p2p behavior p2p
[Router-trafficpolicy-p2p] quit
```

步骤5 在WAN侧三层口GE2/0/0入方向应用流策略

```
[Router] interface gigabitethernet 2/0/0
[Router-GigabitEthernet2/0/0] traffic-policy p2p inbound
[Router-GigabitEthernet2/0/0] quit
```

步骤6 通过**display current-configuration**命令验证配置结果

----结束

配置文件

- Router的配置文件

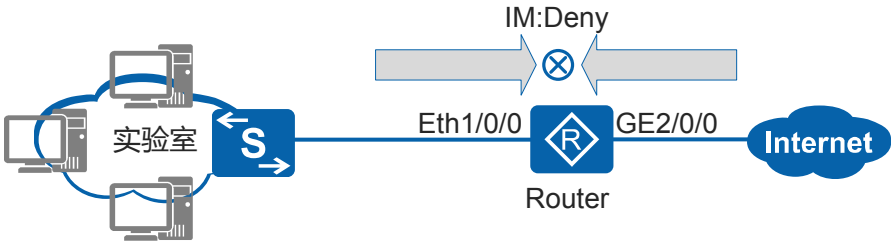
```
#
 sysname Router
#
traffic classifier p2p operator or
 if-match category FileShare_P2P
#
traffic behavior p2p
 car cir 4096 cbs 770048 pbs 1282048 mode color-blind green pass yellow pass red
discard
#
traffic policy p2p
 classifier p2p behavior p2p
#
interface GigabitEthernet2/0/0
 traffic-policy p2p inbound
#
return
```

11.7.2 配置禁止即时通信软件示例

组网需求

如图11-4所示，某学校实验室通过Router作为网关设备连接到外网。通过禁止使用即时通信软件（比如QQ、MSN等）禁止学生从事与学习无关的事务，保证在实验室的学习投入。

图 11-4 配置禁止即时通信软件示例



配置思路

采用如下思路配置SAC：

1. 开启深度安全防御功能，并加载特征库文件。
2. 配置流分类，通过匹配系统缺省的协议组Instant_Messaging，匹配即时通信软件。
3. 配置流行为，禁止Instant_Messaging报文通过。
4. 配置流策略，将流分类和流行为绑定。
5. 在WAN侧接口入方向应用流策略。

操作步骤

步骤1 开启深度安全防御功能，并加载特征库文件

```
<Huawei> system-view
[Huawei] sysname Router
[Router] engine enable
```

步骤2 配置流分类，通过匹配系统缺省的协议组Instant_Messaging，匹配即时通信软件

```
[Router] traffic classifier im
[Router-classifier-im] if-match category Instant_Messaging
[Router-classifier-im] quit
```

步骤3 配置流行为，对识别出的即时通信软件报文进行过滤

```
[Router] traffic behavior im
[Router-behavior-im] deny
[Router-behavior-im] quit
```

步骤4 配置流策略，将流分类和流行为绑定

```
[Router] traffic policy im
[Router-trafficpolicy-im] classifier im behavior im
[Router-trafficpolicy-im] quit
```

步骤5 在WAN侧三层口GE2/0/0入方向应用流策略

```
[Router] interface gigabitethernet 2/0/0
[Router-GigabitEthernet2/0/0] traffic-policy im inbound
[Router-GigabitEthernet2/0/0] quit
```

步骤6 通过**display current-configuration**命令验证配置结果

----结束

配置文件

- Router的配置文件

```
#
 sysname Router
#

traffic classifier im operator or
 if-match category Instant_Messaging
#
traffic behavior im
 deny
#
traffic policy im
 classifier im behavior im
#
interface GigabitEthernet2/0/0
 traffic-policy im inbound
#
return
```

相关

视频：**禁止使用QQ、MSN等即时通讯软件**