

CloudEngine S5700, S6700 系列交换机 V600R023C00

# 配置指南-QoS

文档版本 02

发布日期 2023-12-01



#### 版权所有 © 华为技术有限公司 2023。 保留一切权利。

非经本公司书面许可,任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部,并不得以任何形式传播。

#### 商标声明



HUAWE和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标,由各自的所有人拥有。

#### 注意

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

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

# 华为技术有限公司

地址: 深圳市龙岗区坂田华为总部办公楼 邮编: 518129

网址: <a href="https://e.huawei.com">https://e.huawei.com</a>

# 目录

1	前言		1
2	QoS 4	宗述	4
3	MOC	配置	7
		简介	
		原理描述	
		配置注意事项	
		10年/100年/00年/00年/00年/00年/00年/00年/00年/00年	
		·····································	
3.	7 应用流	·····································	141
3.	9 维护 I	MQC	143
4	据文iv	过滤配置	144
		<u>は</u> 滤筒介	
		过滤配置注意事项	
		ま于 MQC 的报文过滤	
		- 3 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1	
		配置基于源 MAC 地址控制访问的示例	
5	流量级	· · 计配置	154
		<del>た</del> 计简介	
		充计配置注意事项	
		ま于 MQC 的流量统计	
		配置基于 MQC 的流量统计	
		· 5标记配置	
		<b>■标记简介</b>	
		e标记原理	
		E标记配置注意事项	163
		表于 MQC 的报文重标记	
		配置基于 MQC 的报文重标记	
		<b>定向配置</b>	
		<b>是足凹的量</b> 直定向简介	
7.	・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	<b>赴走门间汀</b>	1//

7.2 报文重定向配置注意事项	178
7.3 配置基于 MQC 的报文重定向	188
7.4 举例: 配置报文重定向到接口	191
7.5 举例: 配置报文重定向到下一跳	
7.6 举例: 配置报文重定向到下一跳与 NQA 联动	
7.7 举例: 配置报文重定向实现路由选路	
8 优先级映射配置	208
8.1 优先级映射简介	208
8.2 优先级映射原理描述	209
8.3 优先级映射配置注意事项	211
8.4 优先级映射缺省配置	225
8.5 配置基于 DiffServ 域的优先级映射	230
8.5.1 配置优先级信任模式	230
8.5.2 配置 DiffServ 域	231
8.5.3 应用 DiffServ 域	231
8.5.4 检查配置结果	232
8.5.5 举例: 配置优先级映射	232
8.6 配置端口优先级	235
8.7 配置本设备发送的协议报文的内部优先级	235
8.8 配置内部优先级与队列的映射关系	236
8.9 配置报文的优先级	236
8.10 优先级映射常见配置错误	237
8.10.1 报文未进入正确队列	237
8.10.2 优先级映射结果不正确	238
9 流量监管、流量整形和接口限速配置	240
9.1 流量监管、流量整形和接口限速简介	240
9.2 流量监管、流量整形和接口限速原理描述	241
9.2.1 流量评估与令牌桶技术	241
9.2.2 流量监管	248
9.2.3 流量整形	249
9.2.4 接口限速	250
9.3 流量监管配置注意事项	251
9.4 流量整形配置注意事项	252
9.5 接口限速配置注意事项	255
9.6 流量监管、流量整形和接口限速缺省配置	257
9.7 配置流量监管	257
9.7.1 配置一级 CAR 的流量监管(MQC 方式)	257
9.7.2 配置二级 CAR 的流量监管	259
9.7.3 检查配置结果	259
9.7.4 举例: 配置一级 CAR 的流量监管(MQC 方式)	260
9.7.5 举例:配置流量监管,对网段的每个 IP 单独限速的示例	265
9.8 配置流量整形	268

9.8.1 配置队列流量整形	268
9.8.2 检查配置结果	268
9.8.3 举例:配置流量整形,对不同业务限速的示例	269
9.8.4 举例:配置基于 DiffServ 域优先级映射的流量整形	272
9.8.5 举例:配置基于信任 802.1p 优先级的流量整形	275
9.9 配置接口限速	277
9.9.1 配置流量监管实现接口限速	277
9.9.2 配置流量整形实现接口限速	278
9.9.3 配置管理网口的流量限速	279
9.9.4 举例: 配置流量监管实现接口限速	279
9.10 配置 QoS 模板	281
9.11 维护流量监管、流量整形和接口限速	281
10 拥塞避免配置	<b>28</b> 3
10.1 拥塞避免简介	283
10.2 拥塞避免原理描述	283
10.2.1 WRED 原理	284
10.2.2 用 CFI 作为内部丢弃优先级原理	285
10.3 拥塞避免配置注意事项	286
10.4 拥塞避免缺省配置	290
10.5 配置 WRED	290
10.6 配置 CFI 作为内部丢弃优先级	291
10.7 检查配置结果	292
10.8 维护拥塞避免	292
10.9 举例:配置 WRED	292
11 拥塞管理配置	297
11.1 拥塞管理简介	297
11.2 拥塞管理原理描述	298
11.3 拥塞管理配置注意事项	301
11.4 拥塞管理缺省配置	303
11.5 配置拥塞管理	303
11.6 (可选)配置缓存管理	304
11.6.1 了解缓存管理	
11.6.2 配置缓存管理的突发模式	
11.6.3 配置缓存空间的大小	
11.6.4 配置队列缓存超限告警功能	
11.6.5 检查配置结果	306
11.7 维护拥塞管理	
11.8 举例: 配置拥塞管理	
11.9 举例:配置拥塞避免和拥塞管理综合示例(PQ+WDRR 调度和 WRED 模板)	
11.10 微突发检测	
11.10.1 配置微突发检测	
11.10.2 检查配置结果	315

12 MPLS QoS 配置	316
12.1 MPLS QoS 简介	
12.2 MPLS QoS 原理描述	
12.3 MPLS QoS 配置注意事项	321
12.4 MPLS QoS 缺省配置	322
12.5 配置 DiffServ 模式	323
12.6 配置优先级映射	324
12.6.1 配置 DiffServ 域	325
12.6.2 应用 DiffServ 域	325
12.7 检查 MPLS QoS 配置结果	326
12.8 举例:配置 MPLS QoS 示例	326

1 前言

# 读者对象

本文档适用于负责管理和维护交换机的网络工程师。您应该熟悉以太网基础知识,且 具有丰富的网络管理经验。此外,您应该非常了解您的网络,包括组网拓扑,已部署 的网络业务等。

# 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	表示如不避免则将会导致死亡或严重伤害的具有高等级风险的危害。
▲ 警告	表示如不避免则可能导致死亡或严重伤害的具有中等级风险的危害。
<u></u> 注意	表示如不避免则可能导致轻微或中度伤害的具有低等级风险的危害。
须知	用于传递设备或环境安全警示信息。如不避免则可能会导致设备损坏、数据丢失、设备性能降低或其他不可预知的结果。 "须知"不涉及人身伤害。
□ 说明	对正文中重点信息的补充说明。 "说明"不是安全警示信息,不涉及人身、设备及环 境伤害信息。

# 命令行格式约定

在本文中可能出现下列命令行格式,它们所代表的含义如下。

格式	意义
粗体	命令行关键字(命令中保持不变、必须 照输的部分)采用 <b>加粗</b> 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 <i>斜体</i> 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。

# 安全约定

#### • 密码配置约定

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

#### • 加密算法约定

目前设备采用的加密算法包括DES、3DES、AES、DSA、RSA、DH、ECDH、HMAC、SHA1、SHA2、MD5,具体采用哪种加密算法请根据场景而定。请优先采用我们的建议,否则会造成无法满足您安全防御的要求。

- 对称加密算法建议使用AES(128位及以上密钥)。
- 非对称加密算法建议使用RSA(3072位及以上密钥),使用非对称算法时, 加密和签名要使用不同的密钥对。
- 数字签名建议使用RSA(3072位及以上密钥)。

- 密钥协商建议使用DH(3072位及以上密钥)或者ECDH(256位及以上密钥)。
- 哈希算法建议使用SHA2(256及以上)。
- HMAC(基于哈希算法的消息验证码)算法建议使用HMAC-SHA2。
- SHA1、SHA2和MD5加密算法是不可逆的,DES、3DES、RSA和AES加密算法是可逆的。
- SSH2.0版本中,使用CBC模式的对称加密算法可能存在数据受到明文恢复攻击而泄露加密传输的内容,因此,在SSH2.0中不建议使用CBC模式对数据加密。
- SSL通过握手在客户端和服务器之间建立会话,完成双方身份的验证、密钥和加密套件的协商,在通信过程中建议使用TLS1.2及以上版本的安全套件。TLS版本中,使用CBC模式的对称加密算法可能存在数据受到明文恢复攻击而泄露加密传输的内容,因此,在TLS版本中不建议使用CBC模式对数据加密。

#### • 个人数据约定

您购买的产品、服务或特性在业务运营或故障定位的过程中将可能获取或使用用户的某些个人数据(如终端用户的MAC地址或IP地址),因此您有义务根据所适用国家的法律制定必要的用户隐私政策并采取足够的措施以确保用户的个人数据受到充分的保护。

本文档中出现的"镜像端口、端口镜像、流镜像、镜像"等相关词汇仅限于为了描述该产品进行检测通信传输中的故障和错误的目的而使用,不涉及采集、处理任何个人数据或任何用户通信内容。

#### • 可靠性设计声明

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

#### 参考标准和协议

请登录**华为网站**,搜索"标准协议顺从表",获取《华为S系列交换机标准协议顺从表》。

# **2** QoS 综述

## QoS 简介

网络的普及和业务的多样化使得网络流量激增,从而加剧网络拥塞,增加转发时延,严重时还会产生丢包,导致业务质量下降甚至不可用。所以,要在网络上开展游戏、视频、直播等多样化业务,就必须解决网络拥塞问题。增加网络的带宽可以解决网络拥塞,但从运营、维护的成本考虑,这是不现实的,最有效的解决方案就是应用一个"有保证"的策略对网络流量进行管理。

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

# DiffServ 模型

需要说明的是,QoS不是某一个具体功能,而是一个方案。例如,网络中的两个主机通信时,中间可能会跨越各种各样的设备。只有当网络中所有设备都遵循统一的QoS服务模型时,才能实现端到端的服务质量保证。目前存在多种QoS服务模型,其中应用最广的是差分服务模型(DiffServ,Differentiated Services)。

DiffServ模型的基本原理是将网络中的流量分成多个类,每个类得到不同的处理,尤其是网络出现拥塞时不同的类会享受不同级别的处理。而同一类的业务在网络中会被聚合起来统一发送,保证相同的时延、抖动、丢包率等QoS指标。

设备可以通过多种条件灵活地对报文进行分类,对不同的报文设置不同的优先级,而其他设备只需要简单地识别报文中的这些优先级,即可进行资源分配和流量控制。

设备支持的QoS技术都是基于DiffServ服务模型的,本文从报文分类方式和提供的QoS服务这两个维度来介绍QoS技术。

# QoS 报文分类方式

由上可知,基于DiffServ模型的QoS的基本原理是将网络中的流量分成多个类,每个类享受不同的处理,从而实现差分服务。本文中的QoS技术提供了如下报文分类的方式:

#### 复杂流分类——MQC流分类

复杂流分类即采用复杂的规则,如由五元组(源地址、源端口号、协议号码、目的地址、目的端口号)对报文进行精细的分类,通过将某些具有相同特征的报文划分为一

类,并为这一类报文提供相同的QoS服务。复杂流分类可以通过模块化QoS命令行MQC(Modular QoS Command-Line Interface)中的流分类实现。MQC包含三个要素,分别是流分类、流行为和流策略,三要素通过下面的方式配合使用完成对流量的处理:

- 1. 配置流分类,定义报文匹配规则。
- 2. 配置流行为,确定报文处理动作。根据不同的流行为,可以实现不同的QoS功能,本文提供了基于MQC的流量统计配置、报文过滤配置的详细配置指南。
- 3. 配置流策略,并将配置好的流分类和流行为绑定到一起后在指定视图下应用流策略。

#### 简单流分类——QoS优先级分类

简单流分类就是指采用简单的规则,根据报文中的某个优先级字段,对报文进行粗略的分类。对于优先级的简单介绍如下:

#### • 外部优先级

又称为报文优先级、QoS优先级,即使用报文中某些特定字段比如VLAN报文的802.1p值、IP报文的DSCP值等记录QoS信息。需要注意的是,设备只可以根据设备内部优先级处理收到的报文,为不同的业务提供不同的QoS服务,所以上述外部优先级在进入设备后会映射为设备内部的优先级。

#### • 内部优先级

又称为服务等级(Class of Service)、PHB行为(Per-Hop Behavior)、本地优先级,支持8种取值,优先级从高到低依次为CS7、CS6、EF、AF4、AF3、AF2、AF1、BE,与出端口的8个队列从高到低依次对应。因此内部优先级决定了报文在设备内部所属的队列。当针对某一个队列配置QoS业务时,即对所有通过该队列转发的报文都设置了相同的QoS服务。

#### ● 丟弃优先级

又称为颜色(Color),是指报文在设备内部的丢弃优先级,用于决定当一个队列发生拥塞时报文的丢弃顺序,对内部优先级与队列的映射关系没有影响,丢弃优先级有3种取值,IEEE定义的优先级从低到高依次为Green、Yellow、Red。缺省情况下,丢弃优先级越高,则队列发生拥塞时,对应优先级的报文会被优先丢弃。

然而报文是否会被优先丢弃实际取决于参数的配置。例如,配置WRED丢弃模板中Green最大只能使用50%缓存,Red最大可以使用100%缓存,则队列发生拥塞时,标记为Green的报文将比标记为Red的报文优先丢弃。

设备在处理QoS业务时,在端口入方向(上行方向)将报文的外部优先级映射到合适的内部优先级和丢弃优先级,在端口出方向(下行方向)将内部优先级和丢弃优先级映射到外部优先级。为了将不同报文进行统一的调度,本文提供了如下方式来介绍如何调整外部与内部优先级的映射关系:

 优先级映射配置:在DiffServ模型中,设备定义了DiffServ域来管理和记录外部优 先级与内部优先级、丢弃优先级之间的映射关系,不同DiffServ域允许有不同的优 先级映射关系。优先级映射通过配置DiffServ域来设定不同的优先级映射关系,从 而实现不同的QoS服务。

#### 复杂流分类与简单流分类的关系

通过复杂流分类也可以对特定的QoS优先级报文进行识别,只是需要以MQC流分类的方式去实现。总而言之,需要配置MQC流分类去实现的报文分类都属于复杂流分类;不需要配置MQC流分类,直接根据报文中的外部优先级映射的内部优先级和丢弃优先级去进行报文分类的就是简单流分类。

# QoS 服务技术

对报文分类后,可以对不同类的报文设置不同的QoS服务,本文介绍的QoS服务技术有:

#### 流量监管、流量整形和接口限速

为了使有限的网络资源更有效的为用户服务,就需要对进入网络设备的业务流量加以限制。流量监管、流量整形和接口限速技术规定了允许通过网络设备的不同业务流量的基本带宽(限速),监督进入网络设备的业务流量速率(测速),当业务流量超过基本带宽(超速)时,将超速的流量进行丢弃或者缓存(惩罚),从而达到限制流量、提高资源使用效率的目的,进而保证更好的为用户提供服务。

- 流量监管:将流量限制在特定的带宽内。当业务流量超过额定带宽时,超过的流量将被丢弃。这样可以防止个别业务或用户无限制地占用带宽。
- 流量整形:是一种主动调整流的输出速率的流控措施,使流量比较平稳地传送给下游设备,避免不必要的报文丢弃和拥塞。与流量监管直接将超速的报文丢弃不同,流量整形可以对超速的报文进行缓存以达到均匀向外发送报文流量的目的。
- 接口限速:是对一个接口上发送或者接收全部报文的总速率进行限制,接口限速可以通过流量监管或流量整形的方式去实现。

#### 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拥塞控制机 制。

#### 拥塞管理

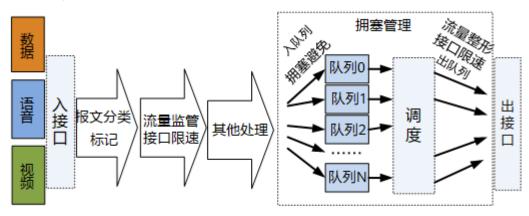
拥塞管理是一项基于队列的技术。当网络发生拥塞时,报文会在队列中缓存,此时拥塞管理会提供某种调度算法安排报文的转发次序,保障一些需要更高质量的QoS服务的业务比如时延敏感业务可以优先调度。

## QoS 业务的处理流程

总而言之,报文分类是为QoS业务提供差分服务的前提和基础;流量监管、流量整形、接口限速、拥塞避免和拥塞管理是从不同方面对网络流量及其分配的资源实施控制,是为QoS业务提供差分服务的具体体现。

QoS业务在网络设备上的处理顺序通常如图2-1所示。

图 2-1 QoS 业务处理流程



# **3** MQC 配置

- 3.1 MQC简介
- 3.2 MQC原理描述
- 3.3 MQC配置注意事项
- 3.4 配置流分类
- 3.5 配置流行为
- 3.6 配置流策略
- 3.7 应用流策略
- 3.8 检查配置结果
- 3.9 维护MQC

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

- 4.3 配置基于MQC的报文过滤
- 配置基于MQC的流量统计
- 6.4 配置基于MQC的报文重标记
- 配置基于MQC的报文重定向

# 3.2 MQC 原理描述

## MQC 三要素

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

#### 流分类

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

- 流分类的名称。
- 流分类的分类规则。设备支持众多的流分类匹配规则,可以分为:链路层规则 (二层规则)、网络层规则(三层规则)、传输层规则(四层规则)、ACL规则 等其他规则。
- 流分类中各规则之间的关系分为: and或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任何一个规则,设备就认为报文属于此类。 以流分类c1为例。流分类c1包括如下规则:
  - ACL规则: 匹配ACL 3000、匹配ACL 3001
  - 非ACL规则: 匹配VLAN ID为10的报文、匹配报文外层Tag的802.1p值为3的 报文

若流分类c1各规则之间的关系为or: 只要报文的VLAN ID为10,或报文外层Tag的802.1p值为3,或报文匹配ACL 3000,或报文匹配ACL 3001,报文就属于流分类c1。

若流分类c1各规则之间的关系为and:只有报文的VLAN ID为10,报文外层Tag的802.1p值为3,且报文匹配ACL 3000或ACL 3001时,报文才属于流分类c1。

#### 流行为

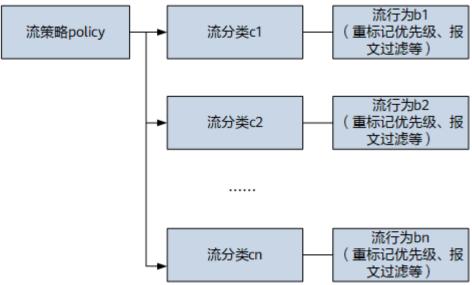
流行为用来定义针对某类报文所做的动作。配置流行为,需要确定如下两点:

- 流行为的名称。
- 流行为中的动作。设备支持报文过滤、重标记优先级、流量统计等动作。如果在一个流行为中定义了多个动作且这些动作互不冲突,那么这些动作都能配置成功且同时生效。如果在一个流行为中定义的多个动作产生冲突,将出现以下情况之一:
  - 在流行为视图定义冲突的动作时,系统提示错误,命令无法执行。
  - 应用流策略时,系统提示错误,流策略应用失败。

#### 流策略

流策略用来将指定的流分类和流行为绑定,对分类后的报文执行对应流行为中定义的动作。如<mark>图3-1</mark>所示,一个流策略可以绑定多个流分类和流行为。

图 3-1 流策略绑定多个流分类和流行为

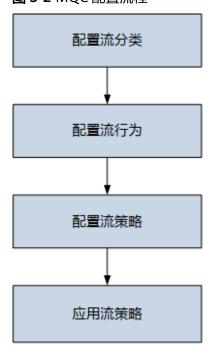


## MQC 配置流程

MQC配置流程如图3-2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:按照需要在相应的视图下应用流策略。

图 3-2 MQC 配置流程



# 3.3 MQC 配置注意事项

# License 依赖

MQC无需License许可即可使用。

# 硬件依赖

表 3-1 支持本特性的硬件

系列	支持产品
S5735-L-V2 series	S5735-L10T4X-A-V2/S5735-L14P2S-QA-V2/S5735-L16LP2UM2X-QA-V2/S5735-L16LP2X-QA-V2/S5735-L16P2UM2X-QA-V2/S5735-L16T4S-A-V2/S5735-L16T4X-QA-V2/S5735-L24P4X-A-V2/S5735-L24P4XE-A-V2/S5735-L24T4X-A-V2/S5735-L24T4X-QA-V2/S5735-L24T4X-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L48LP4S-A-V2/S5735-L48LP4XE-A-V2/S5735-L48S4XE-A-V2/S5735-L48S4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L8P4X-QA-V2/S5735-L8P4X-QA-V2/S5735-L8P4X-QA-V2/S5735-L8T4X-QA-V2
S5735-S-V2 series	S5735-S24HS4XE-V2/S5735-S24P4XE-V2/S5735- S24ST4XE-V2/S5735-S24T4XE-V2/S5735- S24U4XE-V2/S5735-S48HS4XE-V2/S5735- S48P4XE-V2/S5735-S48S4XE-V2/S5735-S48T4XE- V2/S5735-S48U4XE-V2
S5735I-L-V2 series	S5735I-L10T4X-A-V2/S5735I-L8P4X-A-V2
S5755-H series	S5755-H24N4Y-A/S5755-H24P4Y2CZ/S5755- H24T4Y2CZ/S5755-H24U4Y2CZ/S5755- H24UN4Y2CZ/S5755-H24UTM4X4Y2C/S5755- H48N4Y-A/S5755-H48P4Y2CZ/S5755-H48T4Y2CZ/ S5755-H48U4Y2CZ/S5755-H48UN4Y2CZ/S5755- H48UTM4X4Y2C
S6730-H-V2 series	S6730-H24X6C-V2/S6730-H28X6CZ-V2/S6730- H48X6C-V2/S6730-H48X6CZ-V2/S6730-H48Y6C- V2
S5732-H-V2 series	S5732-H24S4X6QZ-V2/S5732-H24UM4Y2CZ-KV2/ S5732-H24UM4Y2CZ-V2/S5732-H44S4X6QZ-V2/ S5732-H48UM4Y2CZ-KV2/S5732-H48UM4Y2CZ- V2
S5735I-H-V2 series	S5735I-H8T4S2XN-V2

系列	支持产品
S5735I-S-V2 series	S5735I-S24T4XE-V2/S5735I-S24U4XE-V2/S5735I- S8T4SN-V2/S5735I-S8T4XN-V2/S5735I-S8U4XN- V2

# 特性限制

表 3-2 本特性的使用限制

特性	特性限制	系列	涉及产品
流类	对于S5735-S-V2 Series/S5735-L-V2 Series/ S5735I-L-V2 Series/S5755-H Series/S6730-H-V2 Series/S5732-H-V2 Series/S5735I-S-V2 Series: 自定义ACL约束: - 仅支持上行应用。 - 不支持与其他规则混合使用。 - 支持应用在全局、端口、VLAN视图。 - 最大解析报文128字节。 - 不支持跟其他字段组合使用。 对于S5735I-H-V2 Series: 自定义ACL约束: - 仅支持上行应用。 - 不支持与其他规则混合使用。	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S5755-H series S6730-H-V2 series S5732-H-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735- S24HS4XE -V2/ S5735- S24P4XE- V2/ S5735- S24ST4XE -V2/ S5735- S24T4XE- V2/ S5735- S24U4XE- V2/ S5735- S48HS4XE -V2/ S5735- S48P4XE- V2/ S5735- S48S4XE- V2/ S5735- S48S4XE- V2/ S5735- S48U4XE- V2/ S5735- S48U4XE- V2/ S5735- S48U4XE- V2/ S5735- S48U4XE- V2/ S5735- S48U4XE- V2/ S5735- S48U4XE- V2/ S5735- L10T4X- A-V2/ S5735- L10T4X- A-V2/ S5735- L16LP2U M2X-QA- V2/ S5735- L16LP2U M2X-QA- V2/ S5735- L16LP2U M2X-QA- V2/ S5735- L16LP2U M2X-QA- V2/ S5735- L16LP2U M2X-QA- V2/ S5735- L16LP2U M2X-QA- V2/ S5735- L16LP2U M2X-QA- V2/ S5735- L16LP2U M2X-QA- V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2UM 2X-QA-

V2/ S5735- L16T4S- A-V2/ S5735- L16T4X- QA-V2/ S5735- L24P4S- A-V2/ S5735- L24P4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L48LP4S- A-V2

特性	特性限制	系列	涉及产品
			L48T4XE- D-V2/ S5735- L8P2T4X- A-V2/ S5735- L8P4S-A- V2/ S5735- L8P4X- QA-V2/ S5735- L8T4S-A- V2/ S5735- L8T4X- QA-V2 S5735I- L10T4X- A-V2/ S5735I- L8P4X-A-
			V2 S5755- H24N4Y- A/S5755- H24P4Y2 CZ/ S5755- H24T4Y2 CZ/ S5755- H24UN4Y 2CZ/ S5755- H24UTM 4X4Y2C/ S5755- H48N4Y- A/S5755- H48P4Y2 CZ/ S5755- H48U4Y2

特性	特性限制	系列	涉及产品
			CZ/ S5755- H48UN4Y 2CZ/ S5755- H48UTM 4X4Y2C
			S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730- H48Y6C- V2
			S5732- H24S4X6 QZ-V2/ S5732- H24UM4 Y2CZ- KV2/ S5732- H24UM4 Y2CZ-V2/ S5732- H44S4X6 QZ-V2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/
			S5735I- S24T4XE- V2/ S5735I- S24U4XE- V2/ S5735I- S8T4SN-

特性	特性限制	系列	涉及产品
			V2/ S5735I- S8T4XN- V2/ S5735I- S8U4XN- V2
			S5735I- H8T4S2X N-V2

特性	特性限制	系列	涉及产品
流类	- 设备最多只能识别到报文的两层tag,如果报文 实际带了三层tag,同样可以命中基于双层Tag进 行分类的匹配规则。	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S5755-H series S6730-H-V2 series S5732-H-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735- S24HS4XE-V2/ S5735- S24P4XE-V2/ S5735- S24ST4XE-V2/ S5735- S24T4XE-V2/ S5735- S24U4XE-V2/ S5735- S48HS4XE-V2/ S5735- S48S4XE-V2/ S5735- S48S4XE-V2/ S5735- S48U4XE-V2/ S5735- S48U4XE-V2/ S5735- L10T4X- A-V2/ S5735- L10T4X- A-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2X- QA-V2/

S5735- L16T4X-  QA-V2/  S5735- L24P4S-  A-V2/  S5735- L24P4XE-  A-V2/  S5735- L24T4XE-  A-V2/  S5735- L24T4X-  A-V2/  S5735- L24T4XE-  A-V2/  S5735- L24T4XE-  A-V2/  S5735- L34T4XE-  A-V2/  S5735- L34BP4S-  A-V2/  S5735- L3BP4XE-  A-V2/  S5735- L3B

特性	特性限制	系列	涉及产品
			S5755- H48UTM 4X4Y2C
			S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730- H48Y6C- V2
			S5732- H24S4X6 QZ-V2/ S5732- H24UM4 Y2CZ- KV2/ S5732- H24UM4 Y2CZ-V2/ S5732- H44S4X6 QZ-V2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/
			S5735I- S24T4XE- V2/ S5735I- S24U4XE- V2/ S5735I- S8T4SN- V2/ S5735I- S8T4XN- V2/

特性	特性限制	系列	涉及产品
			S5735I- S8U4XN- V2
			S5735I- H8T4S2X N-V2

特性	特性限制	系列	涉及产品
流分类	对于S5735-S-V2 Series/S5735-L-V2 Series/ S5735I-L-V2 Series/S5735I-S-V2 Series:	S5735-S- V2 series	S5735- S24HS4XE
	当使用if-match any命令匹配所有的数据报文 时:	S5735-L- V2 series	-V2/ S5735- S24P4XE-
	- 如果流分类是OR关系并且有匹配IPv6 acl ,则 配置if-match any只对对应的IPv6报文生效。	S5735I-L- V2 series	V2/ S5735-
	- if-match any与ARP acl(23000~23999段)规 则同时应用时,if-match any只能对ARP报文生	S5755-H series	S24ST4XE -V2/
	效。 - if-match any与if-match unicast/if-match	S6730-H- V2 series	S5735- S24T4XE- V2/
	unknown-unicast/if-match outbound-interface 规则同时应用时,if-match any只能对非丢弃的 单播和未知单播报文生效。	S5732-H- V2 series	S5735- S24U4XE-
	- if-match any与if-match nexthop规则同时应用时,if-match any只能对非丢弃的三层报文生效。	S5735I-S- V2 series S5735I-H- V2 series	V2/ S5735- S48HS4XE -V2/
	- if-match any与if-match discard规则同时应用 时,if-match any只能对丢弃报文生效。		S5735- S48P4XE-
	- 如果流分类是AND关系,则忽略if-match any规则。		V2/ S5735- S48S4XE-
	对于S5735I-H-V2 Series:		V2/
	当使用if-match any命令匹配所有的数据报文 时:		S5735- S48T4XE- V2/
	对于产品S5735I-H8T4S2XN-V2:		S5735-
	- 如果流分类是OR关系并且有匹配IPv6 acl ,则 配置if-match any只对对应的IPv6报文生效。		S48U4XE- V2
	- if-match any与ARP acl(23000~23999段)规 则同时应用时,if-match any只能对ARP报文生 效。		S5735- L10T4X- A-V2/
	- if-match any与if-match unicast/if-match unknown-unicast/if-match outbound-interface 规则同时应用时,if-match any只能对非丢弃的 单播和未知单播报文生效。		S5735- L14P2S- QA-V2/ S5735- L16LP2U
	- if-match any与if-match nexthop规则同时应用时,if-match any只能对非丢弃的三层报文生效。		M2X-QA- V2/ S5735-
	- if-match any与if-match discard规则同时应用 时,if-match any只能对丢弃报文生效。		L16LP2X- QA-V2/ S5735-
	- 如果流分类是AND关系,则忽略if-match any规则。		L16P2UM 2X-QA-
	对于S5755-H Series/S6730-H-V2 Series/S5732- H-V2 Series:		V2/ S5735-
	当使用if-match any命令匹配所有的数据报文时:		L16T4S- A-V2/

特性	特性限制	系列	涉及产品
	- 如果流分类是OR关系并且有匹配IPv6 acl,则配置if-match any只对对应的IPv6报文生效。 - 如果流分类是OR关系并且有匹配if-match gre、vxlan使用特定ACL模板的规则,则配置if-match any只对特定ACL模板支持的报文类型生效。 - if-match any与ARP acl(23000~23999段)规则同时应用时,if-match any只能对ARP报文生效。 - if-match any与if-match unicast/if-match unknown-unicast/if-match outbound-interface 规则同时应用时,if-match any只能对非丢弃的单播和未知单播报文生效。 - if-match any与if-match nexthop规则同时应用时,if-match any只能对非丢弃的三层报文生效。 - if-match any与if-match discard规则同时应用时,if-match any只能对丢弃报文生效。 - 如果流分类是AND关系,则忽略if-match any规则。		S5735- L16T4X- QA-V2/ S5735- L24P4S- A-V2/ S5735- L24P4XE- A-V2/ S5735- L24T4X- A-V2/ S5735- L24T4X- QA-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- D-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4XE- A-V2/ S5735- L48P4XE- A-V2/ S5735- L48P4XE- A-V2/ S5735- L48P4XE- A-V2/ S5735- L48P4XE- A-V2/ S5735- L48T4S- A-V2/ S5735- L48T4S- A-V2/ S5735- L48T4S- A-V2/ S5735- L48T4S- A-V2/ S5735- L48T4S- A-V2/ S5735- L48T4XE- A-V2/ S5735- L48T4S- A-V2/ S5735- L48T4XE- D-V2/ S5735- L48T4XE- D-V2/ S5735- D-V2/ S5735- D-V2/ S5735- D-V2/ S5735- D-V2/ S5735- D-V2/ S5735- D-V2/ S5735- D-V2/ S573

特性	特性限制	系列	涉及产品
特性	特性限制	系列	A-V2/ S5735- L8P4S-A- V2/ S5735- L8P4X- QA-V2/ S5735- L8T4S-A- V2/ S5735- L8T4X- QA-V2 S5735I- L10T4X- A-V2/ S5735I- L8P4X-A- V2 S5755- H24N4Y- A/S5755- H24P4Y2 CZ/ S5755- H24T4Y2 CZ/ S5755- H24U4Y2 CZ/ S5755- H24U4Y2 CZ/ S5755- H24U4Y2 CZ/
			2CZ/ S5755- H24UTM 4X4Y2C/ S5755- H48N4Y- A/S5755- H48P4Y2 CZ/ S5755- H48T4Y2 CZ/ S5755- H48U4Y2 CZ/ S5755- H48U4Y2 CZ/ S5755- H48UN4Y 2CZ/

特性	特性限制	系列	涉及产品
			S5755- H48UTM 4X4Y2C
			Y2CZ-V2 S5735I- S24T4XE- V2/
			S5735I- S24U4XE- V2/ S5735I- S8T4SN- V2/ S5735I- S8T4XN- V2/

特性	特性限制	系列	涉及产品
			S5735I- S8U4XN- V2
			S5735I- H8T4S2X N-V2

特性	特性限制	系列	涉及产品
流类	对于S5735-S-V2 Series/S5735-L-V2 Series/S5735I-L-V2 Series/S5735I-S-V2 Series/S5735I-H-V2 Series/S5735I-S-V2 Series/S5735I-H-V2 Series: 匹配报文是否丢弃的流分类: - 包含该流分类的流策略不能应用在出方向上。- 根据报文是否丢弃进行流分类时,无法匹配三层转发查表丢弃的报文。	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735- S24HS4XE-V2/ S5735- S24P4XE-V2/ S5735- S24ST4XE-V2/ S5735- S24U4XE-V2/ S5735- S24U4XE-V2/ S5735- S48HS4XE-V2/ S5735- S48S4XE-V2/ S5735- S48C4XE-V2/ S5735- S48U4XE-V2/ S5735- S48U4XE-V2/ S5735- L10T4X- A-V2/ S5735- L10T4X- A-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2X- QA-V2/

S5735- L16T4X- QA-V2/ S5735- L24P4S- A-V2/ S5735- L24P4KE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4S- A-V2/ S5735- L24T4X- QA-V2/ S5735- L24T4X- QA-V2/ S5735- L24T4XE- A-V2/

特性	特性限制	系列	涉及产品
			A-V2/ S5735- L8P4S-A- V2/ S5735- L8P4X- QA-V2/ S5735- L8T4S-A- V2/ S5735- L8T4X- QA-V2 S5735I- L10T4X- A-V2/ S5735I- L8P4X-A-
			V2 S5735I- S24T4XE- V2/ S5735I- S24U4XE- V2/ S5735I- S8T4SN- V2/ S5735I- S8T4XN- V2/ S5735I- S8U4XN- V2 S5735I- S8U4XN- V2

特性	特性限制	系列	涉及产品
流类	流分类规则叠加约束: - 不支持在and模式流分类中同时匹配以下规则: ECN拥塞标记、IP优先级、DSCP优先级、服务优 先级。 - 同一流策略不支持流分类规则同时匹配普通ACL 以及基于ARP的ACL,当需要匹配普通ACL以及基于ARP的ACL时,可以分别在两个流策略中进行应 用。 - 同一个流策略中不支持同时配置匹配IPv4字段和 IPv6字段的规则。	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S5755-H series S6730-H-V2 series S5732-H-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735- S24HS4XE-V2/ S5735- S24P4XE-V2/ S5735- S24ST4XE-V2/ S5735- S24U4XE-V2/ S5735- S24U4XE-V2/ S5735- S48HS4XE-V2/ S5735- S48P4XE-V2/ S5735- S48S4XE-V2/ S5735- S48U4XE-V2/ S5735- S48U4XE-V2/ S5735- L10T4X- A-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16T4S- A-V2/

S5735- L16T4X-  QA-V2/  S5735- L24P4S-  A-V2/  S5735- L24P4XE-  A-V2/  S5735- L24T4XE-  A-V2/  S5735- L24T4X-  A-V2/  S5735- L24T4XE-  A-V2/  S5735- L24T4XE-  A-V2/  S5735- L34T4XE-  A-V2/  S5735- L34BP4S-  A-V2/  S5735- L3BP4XE-  A-V2/  S5735- L3B

特性	特性限制	系列	涉及产品
			S5755- H48UTM 4X4Y2C
			S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730- H48Y6C- V2
			S5732- H24S4X6 QZ-V2/ S5732- H24UM4 Y2CZ- KV2/ S5732- H24UM4 Y2CZ-V2/ S5732- H44S4X6 QZ-V2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/
			S5735I- S24T4XE- V2/ S5735I- S24U4XE- V2/ S5735I- S8T4SN- V2/ S5735I- S8T4XN- V2/

特性	特性限制	系列	涉及产品
			S5735I- S8U4XN- V2
			S5735I- H8T4S2X N-V2

特性	特性限制	系列	涉及产品
流类	对于S5732-H-V2 Series/S5755-H Series/S6730-H-V2 Series: 匹配VXLAN ACL的流分类: - VXLAN ACL不支持匹配DSCP/ECN/IP优先级/TOS。 - VXLAN ACL不支持匹配二层封装类型(etherii、snap)。 - VXLAN ipv6 ACL不支持匹配分片标记。 - if-match vxlan配置对于ipv4/ipv6报文分类仅支持全局、端口、qos group视图。 - if-match vxlan ipv6 acl严格地址模式分类仅支持全局、端口和ipv6 acl严格地址模式分类仅支持全局、端口、三层子接口。二层子接口。二层子接口。二层子接口。二层子接口。二层子接口。二层子接口。二层子接口。二层子接口。二点子按口。二层子接口。二点子按口。一时一个发展,或是一个发展的一个发展的一个发展的一个发展的一个发展的一个发展的一个发展的一个发展的	S5732-H- V2 series S5755-H series S6730-H- V2 series	S5732- H24S4X6 QZ-V2/ S5732- H24UM4 Y2CZ- KV2/ S5732- H24UM4 Y2CZ-V2/ S5732- H44S4X6 QZ-V2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/ S5753- H24N4Y- A/S5755- H24P4Y2 CZ/ S5755- H24UAY2 CZ/ S5755- H24UAY2 CZ/ S5755- H24UTM 4X4Y2C/ S5755- H48N4Y- A/S5755- H48N4Y-

2CZ/ S5755- H48UTM 4X4Y2C S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730- H48Y6C-	特性	特性限制	系列	涉及产品
H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730-				S5755- H48UTM
				S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730-

特性	特性限制	系列	涉及产品
流类	匹配未知单播报文分类的约束:包含该流分类的流策略不能应用在出方向上。	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S5755-H series S6730-H-V2 series S5732-H-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735- S24HS4XE-V2/ S5735- S24P4XE-V2/ S5735- S24ST4XE-V2/ S5735- S24T4XE-V2/ S5735- S24U4XE-V2/ S5735- S48HS4XE-V2/ S5735- S48P4XE-V2/ S5735- S48T4XE-V2/ S5735- S48T4XE-V2/ S5735- S48T4XE-V2/ S5735- S48T4XE-V2/ S5735- S48T4XE-V2/ S5735- S48U4XE-V2/ S5735- S48U4XE-V2/ S5735- S48U4XE-V2/ S5735- S48U4XE-V2/ S5735- L10T4X- A-V2/ S5735- L10T4X- A-V2/ S5735- L10P2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16T4S- A-V2/

特性	特性限制	系列	涉及产品
特性	特性限制	系列	S5735- L16T4X- QA-V2/ S5735- L24P4S- A-V2/ S5735- L24P4XE- A-V2/ S5735- L24ST4XE -A-V2/ S5735- L24T4S- A-V2/ S5735- L24T4X- QA-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/
			A-V2/ S5735- L48LP4XE -A-V2/ S5735- L48P4XE- A-V2/ S5735- L48S4X- A-V2/ S5735- L48T4S- A-V2/ S5735- L48T4XE- D-V2/ S5735- L48T4XE- D-V2/ S5735- L48T4XE- D-V2/ S5735- L48T4XE- D-V2/ S5735- L8P2T4X-

特性	特性限制	系列	涉及产品
			S5755- H48UTM 4X4Y2C
			S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730- H48Y6C-
			V2 S5732- H24S4X6 QZ-V2/ S5732- H24UM4 Y2CZ- KV2/ S5732- H24UM4 Y2CZ-V2/ S5732- H44S4X6 QZ-V2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/ S5732-
			S5735I- S24T4XE- V2/ S5735I- S24U4XE- V2/ S5735I- S8T4SN- V2/ S5735I- S8T4XN- V2/

特性	特性限制	系列	涉及产品
			S5735I- S8U4XN- V2
			S5735I- H8T4S2X N-V2

特性	特性限制	系列	涉及产品
流类	ACL logging报文约束: - 对于上送CPU的协议报文和从CPU发送的报文 logging功能无法保障生效,其他业务优先生效。 - 仅能记录logging上送成功的报文,超过CAR限速值(默认128pps)而被丢弃的报文无法记录。	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S5755-H series S6730-H-V2 series S5732-H-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735- S24HS4XE-V2/ S5735- S24P4XE-V2/ S5735- S24ST4XE-V2/ S5735- S24U4XE-V2/ S5735- S24U4XE-V2/ S5735- S48HS4XE-V2/ S5735- S48P4XE-V2/ S5735- S48S4XE-V2/ S5735- S48U4XE-V2/ S5735- S48U4XE-V2/ S5735- S48U4XE-V2/ S5735- L10T4X- A-V2/ S5735- L10T4X- A-V2/ S5735- L10T4X- A-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2X- QA-V2/

特性	特性限制	系列	涉及产品
特性	特性限制	系列	S5735- L16T4X- QA-V2/ S5735- L24P4S- A-V2/ S5735- L24P4XE- A-V2/ S5735- L24T4S- A-V2/ S5735- L24T4X- QA-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- D-V2/ S5735- L24T4XE- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4XE- A-V2/ S5735- L48LP4XE- A-V2/ S5735- L48S4X- S5735- S
			S5735- L48T4XE- D-V2/ S5735- L8P2T4X-

特性	特性限制	系列	涉及产品
			S5755- H48UTM 4X4Y2C
			S24T4XE- V2/ S5735I- S24U4XE- V2/ S5735I- S8T4SN- V2/
			S5735I- S8T4XN- V2/

特性	特性限制	系列	涉及产品
			S5735I- S8U4XN- V2
			S5735I- H8T4S2X N-V2

特性	特性限制	系列	涉及产品
流类	包含ARP ACL的流策略不能应用在出方向上。	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S5755-H series S6730-H-V2 series S5732-H-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735- S24HS4XE -V2/ S5735- S24P4XE- V2/ S5735- S24ST4XE -V2/ S5735- S24T4XE- V2/ S5735- S24U4XE- V2/ S5735- S48HS4XE -V2/ S5735- S48P4XE- V2/ S5735- S48S4XE- V2/ S5735- S48T4XE- V2/ S5735- S48T4XE- V2/ S5735- S48T4XE- V2/ S5735- S48T4XE- V2/ S5735- S48U4XE- V2/ S5735- L10T4X- A-V2/ S5735- L10T4X- A-V2/ S5735- L16P2U M2X-QA- V2/ S5735- L16P2X- QA-V2/ S5735- L16P2UM 2X-QA- V2/ S5735- L16P2X- QA-V2/ S5735- L16P2X- QA-V2/ S5735- L16P2X- QA-V2/ S5735- L16P2X- QA-V2/ S5735- L16P2UM 2X-QA- V2/ S5735- L16T4S- A-V2/

S5735- L16T4X-  QA-V2/  S5735- L24P4S-  A-V2/  S5735- L24P4XE-  A-V2/  S5735- L24T4XE-  A-V2/  S5735- L24T4X-  A-V2/  S5735- L24T4XE-  A-V2/  S5735- L24T4XE-  A-V2/  S5735- L34T4XE-  A-V2/  S5735- L34BP4S-  A-V2/  S5735- L3BP4XE-  A-V2/  S5735- L3B

特性	特性限制	系列	涉及产品
			S5755- H48UTM 4X4Y2C
			S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730- H48Y6C- V2
			S5732- H24S4X6 QZ-V2/ S5732- H24UM4 Y2CZ- KV2/ S5732- H24UM4 Y2CZ-V2/ S5732- H44S4X6 QZ-V2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/
			S5735I- S24T4XE- V2/ S5735I- S24U4XE- V2/ S5735I- S8T4SN- V2/ S5735I- S8T4XN- V2/

特性	特性限制	系列	涉及产品
			S5735I- S8U4XN- V2
			S5735I- H8T4S2X N-V2

特性	特性限制	系列	涉及产品
A 流类	对于S5732-H-V2 Series/S5755-H Series/S6730-H-V2 Series:  1、无法支持二层信息匹配,即无法匹配mac信息,eth-type,snap、ether-ii信息。  2、头节点和终结节点支持内层报文匹配,无法支持外层报文匹配。	S5732-H-V2 series S5755-H series S6730-H-V2 series	S5732- H24S4X6 QZ-V2/ S5732- H24UM4 Y2CZ- KV2/ S5732- H24UM4 Y2CZ-V2/ S5732- H44S4X6 QZ-V2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/ S5755- H24N4Y- A/S5755- H24P4Y2 CZ/ S5755- H24UHY2 CZ/ S5755- H24UN4Y 2CZ/ S5755- H48N4Y- A/S5755- H48N4Y- A/S5755- H48UN4Y CZ/ S5755- H48UN4Y

2CZ/ S5755- H48UTM 4X4Y2C S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730- H48Y6C-	特性	特性限制	系列	涉及产品
H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730-				S5755- H48UTM
				S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730-

特性	特性限制	系列	涉及产品
流类	匹配IPv4 ACL的流分类: - 如果流策略匹配了TCP、UDP端口号或者分片标记,并且应用在出方向,则可能对分片报文误匹配。 - 通过硬件转发的流量,在流分类中匹配带vpn-instance的ACL规则时,会忽略其中的vpn-instance字段,即公网流量和私网流量都会匹配。若需要精确匹配私网流量,请在对应的三层接口上应用流策略。 - 不支持ttl字段。 - 同一个流策略中IPv4报文的字段和IPv6报文字段不能同时配置。	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S6730-H-V2 series S5732-H-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735- S24HS4XE-V2/ S5735- S24P4XE-V2/ S5735- S24ST4XE-V2/ S5735- S24T4XE-V2/ S5735- S24U4XE-V2/ S5735- S48HS4XE-V2/ S5735- S48S4XE-V2/ S5735- S48S4XE-V2/ S5735- S48U4XE-V2/ S5735- S48U4XE-V2/ S5735- S48U4XE-V2/ S5735- L10T4X- A-V2/ S5735- L10T4X- A-V2/ S5735- L10T4X- A-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2X- S745- S75- S75- S75- S75- S75- S75- S75- S7

特性	特性限制	系列	涉及产品
特性	特性限制	系列	S5735- L16T4X- QA-V2/ S5735- L24P4S- A-V2/ S5735- L24P4XE- A-V2/ S5735- L24ST4XE -A-V2/ S5735- L24T4S- A-V2/ S5735- L24T4X- QA-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/
			A-V2/ S5735- L48LP4XE -A-V2/ S5735- L48P4XE- A-V2/ S5735- L48S4X- A-V2/ S5735- L48T4S- A-V2/ S5735- L48T4XE- D-V2/ S5735- L48T4XE- D-V2/ S5735- L48T4XE- D-V2/ S5735- L48T4XE- D-V2/ S5735- L8P2T4X-

特性	特性限制	系列	涉及产品
			S5755- H48UTM 4X4Y2C
			S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730- H48Y6C- V2
			S5732- H24S4X6 QZ-V2/ S5732- H24UM4 Y2CZ- KV2/ S5732- H24UM4 Y2CZ-V2/ S5732- H44S4X6 QZ-V2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/
			S5735I- S24T4XE- V2/ S5735I- S24U4XE- V2/ S5735I- S8T4SN- V2/ S5735I- S8T4XN- V2/

特性	特性限制	系列	涉及产品
			S5735I- S8U4XN- V2 S5735I- H8T4S2X N-V2
流分类	对于S5735I-H-V2 Series: 匹配IPv6 ACL的流分类: - 入方向应用IPv6 ACL不支持vlan-mapping、vlan-stacking、remark 8021p inner-8021p、remark qos-local-id inbound-match动作。 - 出方向应用IPv6 ACL不支持vlan-stacking、remark qos-local-id动作。 - 协议类型只支持tcp/udp/icmpv6/ipv6/ospf。 - 同一个流策略中不支持和ipv4 acl同时配置。 - 在流分类中匹配带vpn-instance的ACL规则时,会忽略其中的vpn-instance字段,即公网流量和私网流量都会匹配。若需要精确匹配私网流量,请在对应的三层接口上应用流策略。	S5735I-H- V2 series	S5735I- H8T4S2X N-V2

特性	特性限制	系列	涉及产品
流类	匹配外层8021p 0,对于untag报文也会生效。	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S5755-H series S6730-H-V2 series S5732-H-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735- S24HS4XE-V2/ S5735- S24P4XE-V2/ S5735- S24ST4XE-V2/ S5735- S24U4XE-V2/ S5735- S24U4XE-V2/ S5735- S48HS4XE-V2/ S5735- S48S4XE-V2/ S5735- S48S4XE-V2/ S5735- S48U4XE-V2/ S5735- L10T4X- A-V2/ S5735- L10T4X- A-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2X- QA-V2/

S5735- L16T4X-  QA-V2/  S5735- L24P4S-  A-V2/  S5735- L24P4XE-  A-V2/  S5735- L24T4XE-  A-V2/  S5735- L24T4X-  A-V2/  S5735- L24T4XE-  A-V2/  S5735- L24T4XE-  A-V2/  S5735- L34T4XE-  A-V2/  S5735- L34BP4S-  A-V2/  S5735- L3BP4XE-  A-V2/  S5735- L3B

特性	特性限制	系列	涉及产品
特性	特性限制	系列	おいて
			CZ/ S5755- H48U4Y2 CZ/ S5755- H48UN4Y 2CZ/

特性	特性限制	系列	涉及产品
特性	特性限制	系列	S5755- H48UTM 4X4Y2C S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730- H48X6CZ- V2/ S6730- H48X6CZ- V2/ S6730- H48Y6C- V2/ S6730-
			H24S4X6 QZ-V2/ S5732- H24UM4 Y2CZ- KV2/ S5732- H24UM4 Y2CZ-V2/ S5732- H44S4X6 QZ-V2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ-
			S5735I- S24T4XE- V2/ S5735I- S24U4XE- V2/ S5735I- S8T4SN- V2/ S5735I- S8T4XN- V2/

特性	特性限制	系列	涉及产品
			S5735I- S8U4XN- V2
			S5735I- H8T4S2X N-V2

特性	特性限制	系列	涉及产品
流行为	流量限速(CAR): - 应用在跨板LAG、VLAN或跨芯片LAG、VLAN的场景,限速是按照芯片分别限制,实际流量为配置值与芯片个数的乘积。	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S5755-H series S6730-H-V2 series S5732-H-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735- S24HS4XE-V2/ S5735- S24P4XE-V2/ S5735- S24ST4XE-V2/ S5735- S24T4XE-V2/ S5735- S24U4XE-V2/ S5735- S48HS4XE-V2/ S5735- S48S4XE-V2/ S5735- S48S4XE-V2/ S5735- S48T4XE-V2/ S5735- S48U4XE-V2/ S5735- S48U4XE-V2/ S5735- L10T4X- A-V2/ S5735- L10T4X- A-V2/ S5735- L10T4X- A-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2X- S745- S75- S75- S75- S75- S75- S75- S75- S7

特性	特性限制	系列	涉及产品
特性	特性限制	系列	S5735- L16T4X- QA-V2/ S5735- L24P4S- A-V2/ S5735- L24P4XE- A-V2/ S5735- L24T4S- A-V2/ S5735- L24T4X- QA-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- D-V2/ S5735- L24T4XE- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4XE- A-V2/ S5735- L48LP4XE- A-V2/ S5735- L48S4X- S5735- S
			S5735- L48T4XE- D-V2/ S5735- L8P2T4X-

特性	特性限制	系列	涉及产品
			S5755- H48UTM 4X4Y2C
			S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730- H48Y6C- V2
			S5732- H24S4X6 QZ-V2/ S5732- H24UM4 Y2CZ- KV2/ S5732- H24UM4 Y2CZ-V2/ S5732- H44S4X6 QZ-V2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/
			S5735I- S24T4XE- V2/ S5735I- S24U4XE- V2/ S5735I- S8T4SN- V2/ S5735I- S8T4XN- V2/

特性	特性限制	系列	涉及产品
			S5735I- S8U4XN- V2
			S5735I- H8T4S2X N-V2

特性	特性限制	系列	涉及产品
流为	出方向配置流镜像,如果同时配置car,则只能镜像car后的报文。	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S6730-H-V2 series S5732-H-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735- S24HS4XE -V2/ S5735- S24P4XE- V2/ S5735- S24ST4XE -V2/ S5735- S24T4XE- V2/ S5735- S24U4XE- V2/ S5735- S48HS4XE -V2/ S5735- S48P4XE- V2/ S5735- S48S4XE- V2/ S5735- S48U4XE- V2/ S5735- L10T4X- A-V2/ S5735- L10T4X- A-V2/ S5735- L16LP2U M2X-QA- V2/ S5735- L16LP2X- QA-V2/

S5735- L16T4X-  QA-V2/  S5735- L24P4S-  A-V2/  S5735- L24P4XE-  A-V2/  S5735- L24T4XE-  A-V2/  S5735- L24T4X-  A-V2/  S5735- L24T4XE-  A-V2/  S5735- L24T4XE-  A-V2/  S5735- L34T4XE-  A-V2/  S5735- L34BP4S-  A-V2/  S5735- L3BP4XE-  A-V2/  S5735- L3B

特性	特性限制	系列	涉及产品
			S5755- H48UTM 4X4Y2C
			S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730- H48Y6C-
			V2 S5732- H24S4X6 QZ-V2/ S5732- H24UM4 Y2CZ- KV2/ S5732- H24UM4 Y2CZ-V2/ S5732- H44S4X6 QZ-V2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/ S5732-
			S5735I- S24T4XE- V2/ S5735I- S24U4XE- V2/ S5735I- S8T4SN- V2/ S5735I- S8T4XN- V2/

特性	特性限制	系列	涉及产品
			S5735I- S8U4XN- V2
			S5735I- H8T4S2X N-V2
流行 为	对于S5735I-H-V2 Series: 流行为为禁止MAC地址学习时: - 入方向支持的匹配规则范围: 端口号、源 MAC、目的MAC、VLAN、802.1p、tagnum、 IPv4五元组、IPv4 ToS/DSCP/IP precedence、IP fragment。	S5735I-H- V2 series	S5735I- H8T4S2X N-V2

特性	特性限制	系列	涉及产品
流为	对于S5735I-H-V2 Series: 报文过滤动作: - 流分类引用的ACL中rule配置了deny或者流行为中配置了deny动作,相应命中的流量都会被deny。 对于S5735-S-V2 Series/S5735-L-V2 Series/ S5735I-L-V2 Series/S5755-H Series/S6730-H-V2 Series/S5732-H-V2 Series/S5735I-S-V2 Series: 报文过滤动作: - 流分类引用的ACL中rule配置了deny或者流行为中配置了deny动作,相应命中的流量都会被deny。 - Deny动作和其他流动作互斥,即使配置其他动作也不会生效(MAC地址不学习、流量统计和流镜像除外)。	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S5755-H series S6730-H-V2 series S5732-H-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735- S24HS4XE -V2/ S5735- S24P4XE- V2/ S5735- S24ST4XE -V2/ S5735- S24T4XE- V2/ S5735- S24U4XE- V2/ S5735- S48HS4XE -V2/ S5735- S48S4XE- V2/ S5735- S48S4XE- V2/ S5735- S48U4XE- V2/ S5735- S48T4XE- V2/ S5735- S48T4XE- V2/ S5735- S48T4XE- V2/ S5735- S48U4XE- V2/ S5735- L10T4X- A-V2/ S5735- L10T4X- A-V2/ S5735- L16LP2U M2X-QA- V2/ S5735- L16LP2X- QA-V2/

S5735- L16T4X-  QA-V2/  S5735- L24P4S-  A-V2/  S5735- L24P4XE-  A-V2/  S5735- L24T4XE-  A-V2/  S5735- L24T4X-  A-V2/  S5735- L24T4XE-  A-V2/  S5735- L24T4XE-  A-V2/  S5735- L34T4XE-  A-V2/  S5735- L34BP4S-  A-V2/  S5735- L3BP4XE-  A-V2/  S5735- L3B

特性	特性限制	系列	涉及产品
特性	特性限制	系列	A-V2/ S5735- L8P4S-A- V2/ S5735- L8P4X- QA-V2/ S5735- L8T4S-A- V2/ S5735- L8T4X- QA-V2 S5735I- L10T4X- A-V2/ S5735I- L8P4X-A- V2 S5755- H24N4Y- A/S5755- H24P4Y2 CZ/ S5755- H24U4Y2 CZ/ S5755- H24U4Y2 CZ/ S5755- H24U4Y2 CZ/ S5755- H24U4Y2 CZ/ S5755- H24UM4Y2 CZ/ S5755- H24UM4Y2 CZ/ S5755- H24UM4Y2 CZ/ S5755- H24UM4Y2 CZ/ S5755- H24UM4Y2 CZ/ S5755- H24UM4Y2 CZ/ S5755- H24UM4Y2 CZ/ S5755- H24UM4Y2 CZ/ S5755- H24UM4Y2 CZ/ S5755- H24UM4Y2 CZ/ S5755- H48N4Y- A/S5755- H48P4Y2 CZ/ S5755- H48P4Y2 CZ/ S5755- H48P4Y2 CZ/ S5755- H48V4Y- A/S5755- H48V4Y- A/S5755- H48V4Y- CZ/ S5755- H48V4Y- CZ/ S5755- H48V4Y- A/S5755- H48V4Y- CZ/ S5755- H48V4Y- A/S5755- H48V4Y- CZ/ S5755- H48V4- CZ/ S5755- H48V4- CZ/ S5755- H48V4- CZ/ S5755- H48V4- CZ/ S5755- H48V4- CZ/ S5755- H48V4- CZ/ S5755- H48V4- CZ/ S5755- H48V4- CZ/ S5755- H48V4- CZ/ S5755- H48V4- CZ/ S5755- H48V4- CZ/ S5755- H48V4- CZ/ S5755- H48V4- CZ/ S5755- H48V4- CZ/ S5755- H48V4- CZ/ S5755- H48V4- CZ/ S5755- H48V4- CZ/ S5755- H48V4- CZ/ S5755- CZ
			CZ/ S5755- H48UN4Y 2CZ/

特性	特性限制	系列	涉及产品
			S5755- H48UTM 4X4Y2C
			S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730- H48Y6C- V2
			S5732- H24S4X6 QZ-V2/ S5732- H24UM4 Y2CZ- KV2/ S5732- H24UM4 Y2CZ-V2/ S5732- H44S4X6 QZ-V2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/
			S5735I- S24T4XE- V2/ S5735I- S24U4XE- V2/ S5735I- S8T4SN- V2/ S5735I- S8T4XN- V2/

特性	特性限制	系列	涉及产品
			S5735I- S8U4XN- V2
			S5735I- H8T4S2X N-V2

特性	特性限制	系列	涉及产品
流为	对于S5735-S-V2 Series/S5735-L-V2 Series/S5735I-L-V2 Series/S5735I-S-V2 Series/S5735I-L-V2 Series/S5735I-H-V2 Series: VLAN mapping流行为约束: - 入方向VLAN mapping只支持和deny、permit、mac-address learning disable、remark 8021p、remark qos-local-id同时配置。 - 入方向支持的匹配规则范围: 端口号、源MAC、目的MAC、VLAN、802.1p、tagnum、IPv4五元组、IPv4 ToS/DSCP/IP precedence、IP fragment、ethertype、接口。 - 在流分类中匹配带外层VLAN ID的ACL规则并叠加了VLAN Mapping功能时,入方向和出方向匹配的都是VLAN Mapping映射后的VLAN ID。	S5735-S- V2 series S5735I-L- V2 series S5735I-S- V2 series S5735I-H- V2 series	S5735- S24HS4XE -V2/ S5735- S24P4XE- V2/ S5735- S24ST4XE -V2/ S5735- S24T4XE- V2/ S5735- S24U4XE- V2/ S5735- S48HS4XE -V2/ S5735- S48S4XE- V2/ S5735- S48S4XE- V2/ S5735- S48U4XE- V2/ S5735- S48T4XE- V2/ S5735- S48U4XE- V2/ S5735- S48U4XE- V2/ S5735- L10T4X- A-V2/ S5735- L10T4X- A-V2/ S5735- L16LP2U M2X-QA- V2/ S5735- L16LP2X- QA-V2/

S5735- L16T4X-  QA-V2/  S5735- L24P4S-  A-V2/  S5735- L24P4XE-  A-V2/  S5735- L24T4XE-  A-V2/  S5735- L24T4X-  A-V2/  S5735- L24T4XE-  A-V2/  S5735- L24T4XE-  A-V2/  S5735- L34T4XE-  A-V2/  S5735- L34BP4S-  A-V2/  S5735- L3BP4XE-  A-V2/  S5735- L3B

特性	特性限制	系列	涉及产品
			A-V2/ S5735- L8P4S-A- V2/ S5735- L8P4X- QA-V2/ S5735- L8T4S-A- V2/ S5735- L8T4X- QA-V2 S5735I- L10T4X- A-V2/ S5735I- L8P4X-A- V2 S5735I- S24T4XE- V2/
			S5735I- S24U4XE- V2/ S5735I- S8T4SN- V2/ S5735I- S8T4XN- V2/ S5735I- S8U4XN- V2 S5735I- H8T4S2X N-V2

特性	特性限制	系列	涉及产品
流行	对于S5732-H-V2 Series/S5755-H Series/S6730-H-V2 Series: 禁用URPF功能流行为约束: 仅支持入方向应用。	S5732-H- V2 series S5755-H series S6730-H- V2 series	S5732- H24S4X6 QZ-V2/ S5732- H24UM4 Y2CZ- KV2/ S5732- H24UM4 Y2CZ-V2/ S5732- H44S4X6 QZ-V2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ-V2 S5755- H24N4Y- A/S5755- H24P4Y2 CZ/ S5755- H24UAY2 CZ/ S5755- H24UN4Y 2CZ/ S5755- H48N4Y- A/S5755- H4

2CZ/ S5755- H48UTM 4X4Y2C S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730- H48Y6C-	特性	特性限制	系列	涉及产品
H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730-				S5755- H48UTM
				S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730-

特性	特性限制	系列	涉及产品
	据文的内层报文携带2层VLAN Tag(添加的VLAN Tag和原始VLAN Tag)。 (5)原始报文为二层tag报文,二层子接口允许通过流配置为default,则报文将从该二层子接口进入VXLAN域,且该报文的内层报文携带3层 VLAN Tag(添加的VLAN Tag和原始VLAN Tag)。 (6)原始报文为二层tag报文,二层子接口允许通过流配置为dot1q,则物理接口收到报文后,设备会使用添加的VLAN Tag去匹配二层子接口的配置,如果没有匹配到,则使用报文原来的VLAN Tag去匹配二层子接口的配置。匹配到二层子接口的配置,如果没有吃配到)。 (7)原始报文为二层tag报文,二层子接口允许通过流配置为qinq,则物理接口收到报文后,设备会使用添加的VLAN Tag去匹配二层子接口的配置,如果没有匹配到,则使用报文原来到上层子接口的配置,如果没有匹配到,则使用报文原来到二层子接口后,报文将从该二层子接口进入VXLAN域,且该报文的内层携带3层VLAN Tag(添加的VLAN Tag、原始VLAN Tag)。		S5735- L16T4X- QA-V2/ S5735- L24P4S- A-V2/ S5735- L24P4XE- A-V2/ S5735- L24ST4XE- A-V2/ S5735- L24T4X- QA-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- D-V2/ S5735- L24T4XE- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48P4XE- A-V2/ S5735- L48P4XE- A-V2/ S5735- L48P4XE- A-V2/ S5735- L48P4XE- A-V2/ S5735- L48P4XE- A-V2/ S5735- L48S4X- A-V2/ S5735- L48S4X- A-V2/ S5735- L48T4XE- D-V2/ S5735- L48T4XE- D-V2/ S5735- D-V2/ S5735- D-V2/ S5735- D-V2/ S5735- D-V2/ S5735- D-V2/ S5735- D-V2/ S5735- D-V2/ S5735- D-V2/ S5735- D-V2/ S5735- D-V2/ S5735- D-V2/ S5735- D-V2/ S5735- D-V2/ S5735- D-V2/ S5735- D-V2/ S5735

特性	特性限制	系列	涉及产品
特性	特性限制	系列	A-V2/ S5735- L8P4S-A- V2/ S5735- L8P4X- QA-V2/ S5735- L8T4S-A- V2/ S5735- L8T4X- QA-V2 S5735I- L10T4X- A-V2/ S5735I- L8P4X-A- V2 S5755- H24N4Y- A/S5755- H24P4Y2 CZ/ S5755- H24UN4Y 2CZ/ S5755- H48N4Y- A/S5755- H48P4Y2 CZ/ S5755- H48P4Y2 CZ/ S5755- H48P4Y2 CZ/ S5755- H48P4Y2 CZ/ S5755- H48P4Y2 CZ/ S5755- H48P4Y2 CZ/ S5755- H48P4Y2 CZ/ S5755- H48P4Y2 CZ/
			CZ/ S5755- H48U4Y2 CZ/ S5755- H48UN4Y 2CZ/

特性	特性限制	系列	涉及产品
			S5755- H48UTM 4X4Y2C
			Y2CZ-V2 S5735I- S24T4XE- V2/
			S5735I- S24U4XE- V2/ S5735I- S8T4SN- V2/ S5735I- S8T4XN- V2/

特性	特性限制	系列	涉及产品
			S5735I- S8U4XN- V2

特性	特性限制	系列	涉及产品
流略	对于S5735I-H-V2 Series: 接口下应用流策略: - Eth-trunk接口下应用流策略时,如果有成员接口更新,会触发流策略重新下发,此时会导致已应用的流策略短暂失效。 - 三层主接口应用流策略时仅支持三层单播流量。	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S5755-H series S6730-H-V2 series S5732-H-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735- S24HS4XE -V2/ S5735- S24P4XE- V2/ S5735- S24ST4XE -V2/ S5735- S24U4XE- V2/ S5735- S24U4XE- V2/ S5735- S48HS4XE -V2/ S5735- S48S4XE- V2/ S5735- S48T4XE- V2/ S5735- S48T4XE- V2/ S5735- S48T4XE- V2/ S5735- S48U4XE- V2/ S5735- L10T4X- A-V2/ S5735- L10T4X- A-V2/ S5735- L16LP2U M2X-QA- V2/ S5735- L16LP2U M2X-QA- V2/ S5735- L16LP2X- QA-V2/

A-V2/ S5735- L16T4X- QA-V2/ S5735- L24P4S- A-V2/ S5735- L24P4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4X- QA-V2/ S5735- L24T4X- A-V2/ S5735- L24T4X- QA-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L48LP4XE- A-V2/ S5735- L48LP4XE- A-V2/ S5735- L48P4XE- A-V2/
S5735- L48T4XE-

特性	特性限制	系列	涉及产品
特性	特性限制	系列	L8P2T4X- A-V2/ S5735- L8P4S-A- V2/ S5735- L8P4X- QA-V2/ S5735- L8T4S-A- V2/ S5735- L8T4X- QA-V2 S5735- L10T4X- A-V2/ S5735- L10T4X- A-V2/ S5735- L8P4X-A- V2 S5755- H24N4Y- A/S5755- H24P4Y2 CZ/ S5755- H24UN4Y 2CZ/ S5755- H48N4Y- A/S5755- H48P4Y2 CZ/ S5755- H48P4Y2 CZ/

特性	特性限制	系列	涉及产品
			2CZ/ S5755- H48UTM 4X4Y2C
			S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730- H48Y6C-
			V2 S5732- H24S4X6 QZ-V2/ S5732- H24UM4 Y2CZ- KV2/ S5732- H24UM4 Y2CZ-V2/ S5732- H44S4X6 QZ-V2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/
			Y2CZ-V2 S5735I- S24T4XE- V2/ S5735I- S24U4XE- V2/ S5735I- S8T4SN- V2/ S5735I- S8T4XN-

特性	特性限制	系列	涉及产品
			V2/ S5735I- S8U4XN- V2
			S5735I- H8T4S2X N-V2

特性	特性限制	系列	涉及产品
流略	对于S5732-H-V2 Series/S5755-H Series/S6730-H-V2 Series: VPN实例上应用流策略时: 流分类规则不支持匹配IPv6报文。如果vpn视图配置了双流策略,只能命中一个,第一个流策略优先。	S5732-H- V2 series S5755-H series S6730-H- V2 series	S5732- H24S4X6 QZ-V2/ S5732- H24UM4 Y2CZ- KV2/ S5732- H24UM4 Y2CZ-V2/ S5732- H44S4X6 QZ-V2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/ S5755- H24N4Y- A/S5755- H24P4Y2 CZ/ S5755- H24UAY2 CZ/ S5755- H24UAY2 CZ/ S5755- H24UTM 4X4Y2C/ S5755- H48N4Y- A/S5755- H48N4Y- A/S5

2CZ/ S5755- H48UTM 4X4Y2C S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730- H48Y6C-	特性	特性限制	系列	涉及产品
H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730-				S5755- H48UTM
				S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730-

特性	特性限制	系列	涉及产品
流略	全局视图下应用流策略时: 流策略模板名字不能和关键字atomic-update-mode、chip-based-mode有从首字母开始重叠的情况,如at,atom,chi等,但是可以是abc,cc等名字。	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S5755-H series S6730-H-V2 series S5732-H-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735- S24HS4XE -V2/ S5735- S24P4XE- V2/ S5735- S24ST4XE -V2/ S5735- S24T4XE- V2/ S5735- S24U4XE- V2/ S5735- S48HS4XE -V2/ S5735- S48S4XE- V2/ S5735- S48S4XE- V2/ S5735- S48U4XE- V2/ S5735- S48T4XE- V2/ S5735- S48U4XE- V2/ S5735- L10T4X- A-V2/ S5735- L16LP2U M2X-QA- V2/ S5735- L16LP2U M2X-QA- V2/ S5735- L16LP2U M2X-QA- V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2U M2X-QA- V2/ S5735- L16LP2X- QA-V2/

特性	特性限制	系列	涉及产品
特性	特性限制	系列	S5735- L16T4X- QA-V2/ S5735- L24P4S- A-V2/ S5735- L24P4XE- A-V2/ S5735- L24T4S- A-V2/ S5735- L24T4X- QA-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- D-V2/ S5735- L24T4XE- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4XE- A-V2/ S5735- L48LP4XE- A-V2/ S5735- L48S4X- S5735- S
			S5735- L48T4XE- D-V2/ S5735- L8P2T4X-

特性	特性限制	系列	涉及产品
特性	特性限制	系列	おいて
			CZ/ S5755- H48U4Y2 CZ/ S5755- H48UN4Y 2CZ/

特性	特性限制	系列	涉及产品
			S5755- H48UTM 4X4Y2C
			S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730- H48Y6C- V2
			S5732- H24S4X6 QZ-V2/ S5732- H24UM4 Y2CZ- KV2/ S5732- H24UM4 Y2CZ-V2/ S5732- H44S4X6 QZ-V2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/
			S5735I- S24T4XE- V2/ S5735I- S24U4XE- V2/ S5735I- S8T4SN- V2/ S5735I- S8T4XN- V2/

特性	特性限制	系列	涉及产品
			S5735I- S8U4XN- V2
			S5735I- H8T4S2X N-V2

特性	特性限制	系列	涉及产品
流略	对于S5732-H-V2 Series/S5755-H Series/S6730-H-V2 Series: 三层子接口应用流策略的约束: - 不支持配置端口、VLAN匹配项。 - 子接口如果配置不完备导致应用流策略失败不会打印应用失败提示信息,用户可以通过display traffic-policy applied-record查看应用状态。 - 仅支持三层单播流量。 - 流行为中不建议叠加修改vlan的动作,否则会导致流量因为vlan发生变更而无法正常转发。	S5732-H- V2 series S5755-H series S6730-H- V2 series	S5732- H24S4X6 QZ-V2/ S5732- H24UM4 Y2CZ- KV2/ S5732- H24UM4 Y2CZ-V2/ S5732- H44S4X6 QZ-V2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/ S5755- H24N4Y- A/S5755- H24P4Y2 CZ/ S5755- H24UAY2 CZ/ S5755- H24UTM 4X4Y2C/ S5755- H48N4Y- A/S5755- H48N4Y- A/S575

2CZ/ S5755- H48UTM 4X4Y2C S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730- H48Y6C-	特性	特性限制	系列	涉及产品
H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730-				S5755- H48UTM
				S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730-

特性	特性限制	系列	涉及产品
流略	流策略无法对镜像流量生效。	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S5755-H series S6730-H-V2 series S5732-H-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735- S24HS4XE-V2/ S5735- S24P4XE-V2/ S5735- S24ST4XE-V2/ S5735- S24T4XE-V2/ S5735- S24U4XE-V2/ S5735- S48HS4XE-V2/ S5735- S48S4XE-V2/ S5735- S48S4XE-V2/ S5735- S48T4XE-V2/ S5735- S48U4XE-V2/ S5735- S48U4XE-V2/ S5735- S48U4XE-V2/ S5735- S48U4XE-V2/ S5735- L10T4X- A-V2/ S5735- L10T4X- A-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP3X- QA-V2/ S5735- S735

S5735- L16T4X-  QA-V2/  S5735- L24P4S-  A-V2/  S5735- L24P4XE-  A-V2/  S5735- L24T4XE-  A-V2/  S5735- L24T4X-  A-V2/  S5735- L24T4XE-  A-V2/  S5735- L24T4XE-  A-V2/  S5735- L34T4XE-  A-V2/  S5735- L34BP4S-  A-V2/  S5735- L3BP4XE-  A-V2/  S5735- L3B

特性	特性限制	系列	涉及产品
			S5755- H48UTM 4X4Y2C
			S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730- H48Y6C- V2
			S5732- H24S4X6 QZ-V2/ S5732- H24UM4 Y2CZ- KV2/ S5732- H24UM4 Y2CZ-V2/ S5732- H44S4X6 QZ-V2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/
			S5735I- S24T4XE- V2/ S5735I- S24U4XE- V2/ S5735I- S8T4SN- V2/ S5735I- S8T4XN- V2/

特性	特性限制	系列	涉及产品
			S5735I- S8U4XN- V2
			S5735I- H8T4S2X N-V2

特性	特性限制	系列	涉及产品
流略	对于S5732-H-V2 Series/S5755-H Series/S6730-H-V2 Series: 在二层子接口接入VXLAN的场景中: 流分类不能匹配报文的原始VLAN,也不能在该VLAN外的其他字段,然后在VLAN对应的BD上应用流策略。	S5732-H- V2 series S5755-H series S6730-H- V2 series	S5732- H24S4X6 QZ-V2/ S5732- H24UM4 Y2CZ- KV2/ S5732- H24UM4 Y2CZ-V2/ S5732- H44S4X6 QZ-V2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/ S5755- H24N4Y- A/S5755- H24P4Y2 CZ/ S5755- H24UAY2 CZ/ S5755- H24UN4Y 2CZ/ S5755- H48N4Y- A/S5755- H

2CZ/ S5755- H48UTM 4X4Y2C S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730- H48Y6C-	特性	特性限制	系列	涉及产品
H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730-				S5755- H48UTM
				S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730-

特性	特性限制	系列	涉及产品
流略	对于由于配置了本机防攻击功能而丢弃的报文,设备上配置的流策略不生效。	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S5755-H series S6730-H-V2 series S5732-H-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735- S24HS4XE-V2/ S5735- S24P4XE-V2/ S5735- S24ST4XE-V2/ S5735- S24U4XE-V2/ S5735- S24U4XE-V2/ S5735- S48HS4XE-V2/ S5735- S48S4XE-V2/ S5735- S48S4XE-V2/ S5735- S48U4XE-V2/ S5735- S48U4XE-V2/ S5735- S48U4XE-V2/ S5735- L10T4X- A-V2/ S5735- L14P2S- QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2X- QA-V2/

特性	特性限制	系列	涉及产品
特性	特性限制	系列	S5735- L16T4X- QA-V2/ S5735- L24P4S- A-V2/ S5735- L24P4XE- A-V2/ S5735- L24ST4XE -A-V2/ S5735- L24T4S- A-V2/ S5735- L24T4X- QA-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/
			A-V2/ S5735- L48LP4XE -A-V2/ S5735- L48P4XE- A-V2/ S5735- L48S4X- A-V2/ S5735- L48T4S- A-V2/ S5735- L48T4XE- D-V2/ S5735- L48T4XE- D-V2/ S5735- L48T4XE- D-V2/ S5735- L48T4XE- D-V2/ S5735- L8P2T4X-

特性	特性限制	系列	涉及产品
			S5755- H48UTM 4X4Y2C
			S24T4XE- V2/ S5735I- S24U4XE- V2/ S5735I- S8T4SN- V2/
			S5735I- S8T4XN- V2/

特性	特性限制	系列	涉及产品
			S5735I- S8U4XN- V2
			S5735I- H8T4S2X N-V2

特性	特性限制	系列	涉及产品
流略	流策略资源使用情况: - 应用流策略需要设备有足够的ACL资源,否则会导致应用失败,具体占用ACL资源情况视配置情况决定: 1)流分类中配置了if-match acl、if-match ipv6 acl,通常情况下acl组中单条rule占用1条acl资源,如果rule中配置了4层端口号range,则该条rule会做拆分,具体拆分条目数可以基于命令行display system tcam acl port-division查询。如果rule中配置了tcp-flag established,该rule占用2条ACL资源。如果rule引用ip pool、4层端口号pool,则该rule占用acl资源数目视pool配置情况决定。 2)流分类中配置了if-match vlan/inner-vlan,占用ACL资源数目受vlan ID配置范围影响,具体拆分条目可以基于命令行display system tcam acl port-division查询。 3)流分类中配置了if-match的匹配项可以同时指定多个数值,如if-match 8021p 2 3,则ACL资源占用个数和数值个数相同。 4)流策略AND和OR的模式影响ACL资源占用,AND模式时,除if-match acl/ipv6 acl外,其他if-match匹配项会和acl中rule做合并处理,例如:流分类中配置if-match acl 3000和if-match source-mac,其中acl 3000中配置有3条rule(假设最终拆分后是3条,而OR模式则是占用4条。if)如:流分类中配置if-match acl 3000和if-match vlan 1 to 2,其中acl 3000中配置有3条rule(假设最终拆分后是3条规则),vlan 1 to 2拆分后是占用2条,则AND模式下占用ACL资源是3*2=6条(同一条流无法同时两足比资源是3*2=6条(同一条流无法同时两足比资源是3*2=6条(同一条流无法同时两足比资源是3*2=6条(同一条流无法同时两足以则最终拆分结果就是vlan 1和acl中vlac合并生成另外3条),而OR模式则是占用5条。	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S5755-H series S6730-H-V2 series S5732-H-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735- S24HS4XE-V2/ S5735- S24P4XE-V2/ S5735- S24ST4XE-V2/ S5735- S24T4XE-V2/ S5735- S24U4XE-V2/ S5735- S48HS4XE-V2/ S5735- S48P4XE-V2/ S5735- S48S4XE-V2/ S5735- S48T4XE-V2/ S5735- S48T4XE-V2/ S5735- S48U4XE-V2/ S5735- S48U4XE-V2/ S5735- L10T4X- A-V2/ S5735- L10T4X- A-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP3X- S735

特性	特性限制	系列	涉及产品
特性	特性限制	系列	S5735- L16T4X- QA-V2/ S5735- L24P4S- A-V2/ S5735- L24P4XE- A-V2/ S5735- L24T4S- A-V2/ S5735- L24T4X- QA-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- D-V2/ S5735- L24T4XE- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4XE- A-V2/ S5735- L48LP4XE- A-V2/ S5735- L48S4X- S5735- S
			S5735- L48T4XE- D-V2/ S5735- L8P2T4X-

特性	特性限制	系列	涉及产品
			S5755- H48UTM 4X4Y2C
			S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730- H48Y6C- V2
			S5732- H24S4X6 QZ-V2/ S5732- H24UM4 Y2CZ- KV2/ S5732- H24UM4 Y2CZ-V2/ S5732- H44S4X6 QZ-V2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/
			S5735I- S24T4XE- V2/ S5735I- S24U4XE- V2/ S5735I- S8T4SN- V2/ S5735I- S8T4XN- V2/

特性	特性限制	系列	涉及产品
			S5735I- S8U4XN- V2
			S5735I- H8T4S2X N-V2

特性	特性限制	系列	涉及产品
流略	对于S5732-H-V2 Series/S5755-H Series/S6730-H-V2 Series: 三层LAG子接口应用流策略约束: - 三层LAG子接口下应用流策略时,如果LAG口无成员,则会报子接口配置不完备。	S5732-H- V2 series S5755-H series S6730-H- V2 series	S5732- H24S4X6 QZ-V2/ S5732- H24UM4 Y2CZ- KV2/ S5732- H24UM4 Y2CZ-V2/ S5732- H44S4X6 QZ-V2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/ S5755- H24N4Y- A/S5755- H24P4Y2 CZ/ S5755- H24UTM 4X4Y2C/ S5755- H48N4Y- A/S5755- H48N4Y- A/S5755- H48N4Y- A/S5755- H48UAY2 CZ/ S5755- H48UAY2 CZ/ S5755- H48UAY2 CZ/ S5755- H48UN4Y

特性	特性限制	系列	涉及产品
			2CZ/ S5755- H48UTM 4X4Y2C
			S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ-
			V2/ S6730- H48Y6C- V2

特性	特性限制	系列	涉及产品
流略	查询规则命中信息的约束: - 命令行display system tcam match-rules需要遍历获取所有规则统计信息,当acl应用的规格较大时,存在若干秒的显示时延,请等待。	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S5755-H series S6730-H-V2 series S5732-H-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735- S24HS4XE -V2/ S5735- S24P4XE- V2/ S5735- S24ST4XE -V2/ S5735- S24T4XE- V2/ S5735- S24U4XE- V2/ S5735- S48HS4XE -V2/ S5735- S48S4XE- V2/ S5735- S48S4XE- V2/ S5735- S48U4XE- V2/ S5735- S48T4XE- V2/ S5735- S48T4XE- V2/ S5735- S48T4XE- V2/ S5735- S48U4XE- V2/ S5735- L10T4X- A-V2/ S5735- L10T4X- A-V2/ S5735- L16LP2U M2X-QA- V2/ S5735- L16LP2X- QA-V2/

特性	特性限制	系列	涉及产品
特性	特性限制	系列	S5735- L16T4X- QA-V2/ S5735- L24P4S- A-V2/ S5735- L24P4XE- A-V2/ S5735- L24ST4XE -A-V2/ S5735- L24T4S- A-V2/ S5735- L24T4X- QA-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/
			A-V2/ S5735- L48LP4XE -A-V2/ S5735- L48P4XE- A-V2/ S5735- L48S4X- A-V2/ S5735- L48T4S- A-V2/ S5735- L48T4XE- D-V2/ S5735- L48T4XE- D-V2/ S5735- L48T4XE- D-V2/ S5735- L48T4XE- D-V2/ S5735- L8P2T4X-

特性	特性限制	系列	涉及产品
特性	特性限制	系列	S5755- H48UTM 4X4Y2C S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730- H48X6CZ- V2/ S6730- H48X6CZ- V2/ S6730- H48Y6C- V2/ S6730-
			H24S4X6 QZ-V2/ S5732- H24UM4 Y2CZ- KV2/ S5732- H24UM4 Y2CZ-V2/ S5732- H44S4X6 QZ-V2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ-
			S5735I- S24T4XE- V2/ S5735I- S24U4XE- V2/ S5735I- S8T4SN- V2/ S5735I- S8T4XN- V2/

特性	特性限制	系列	涉及产品
			S5735I- S8U4XN- V2
			S5735I- H8T4S2X N-V2

特性	特性限制	系列	涉及产品
流略	应用流策略或者修改、删除已应用流策略的数据时,配置的实际生效时间相对配置提交时间会有延时,规则数量越多,延迟越长。在极端情况下,配置生效的延迟时间可能达到分钟级。	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S5755-H series S6730-H-V2 series S5732-H-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735- S24HS4XE-V2/ S5735- S24P4XE-V2/ S5735- S24ST4XE-V2/ S5735- S24U4XE-V2/ S5735- S24U4XE-V2/ S5735- S48HS4XE-V2/ S5735- S48S4XE-V2/ S5735- S48U4XE-V2/ S5735- S48U4XE-V2/ S5735- S48U4XE-V2/ S5735- S48U4XE-V2/ S5735- S48U4XE-V2/ S5735- S48U4XE-V2/ S5735- L10T4X- A-V2/ S5735- L10T4X- A-V2/ S5735- L10T4X- A-V2/ S5735- L10T4X- A-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2X- QA-V2/

S5735- L16T4X-  QA-V2/  S5735- L24P4S-  A-V2/  S5735- L24P4XE-  A-V2/  S5735- L24T4XE-  A-V2/  S5735- L24T4X-  A-V2/  S5735- L24T4XE-  A-V2/  S5735- L24T4XE-  A-V2/  S5735- L34T4XE-  A-V2/  S5735- L34BP4S-  A-V2/  S5735- L3BP4XE-  A-V2/  S5735- L3B

特性	特性限制	系列	涉及产品
特性	特性限制	系列	A-V2/ S5735- L8P4S-A- V2/ S5735- L8P4X- QA-V2/ S5735- L8T4S-A- V2/ S5735- L10T4X- A-V2/ S5735I- L10T4X- A-V2/ S5735I- L8P4X-A- V2 S5755- H24N4Y- A/S5755- H24P4Y2 CZ/ S5755- H24UN4Y CZ/ S5755- H24UN4Y 2CZ/ S5755- H24UN4Y A/S5755- H48N4Y- A/S5755- H48N4Y- A/S5755- H48P4Y2 CZ/ S5755- H48P4Y2
			CZ/ S5755-

特性	特性限制	系列	涉及产品
			S5755- H48UTM 4X4Y2C
			S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730- H48Y6C- V2
			S5732- H24S4X6 QZ-V2/ S5732- H24UM4 Y2CZ- KV2/ S5732- H24UM4 Y2CZ-V2/ S5732- H44S4X6 QZ-V2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/
			S5735I- S24T4XE- V2/ S5735I- S24U4XE- V2/ S5735I- S8T4SN- V2/ S5735I- S8T4XN- V2/

特性	特性限制	系列	涉及产品
			S5735I- S8U4XN- V2
			S5735I- H8T4S2X N-V2

特性	特性限制	系列	涉及产品
流略	对于S5735I-H-V2 Series: VLANIF接口下应用流策略时: - 不支持VRRP等叠加业务的场景。 - 不支持配置目的MAC地址分类。 - 仅支持三层单播流量。 对于S5735I-L-V2 Series/S5735-L-V2 Series/S5735I-L-V2 Series/S5735I-S-V2 Series: VLANIF接口下应用流策略时: - 不支持VRRP等叠加业务的场景。 - 不支持配置目的MAC地址分类。 - 仅支持三层单播流量。 - 流行为中不建议叠加修改vlan的动作,否则导致因为vlan发生变更无法正常转发。	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S5755-H series S6730-H-V2 series S5732-H-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735- S24HS4XE-V2/ S5735- S24P4XE-V2/ S5735- S24ST4XE-V2/ S5735- S24T4XE-V2/ S5735- S24U4XE-V2/ S5735- S48HS4XE-V2/ S5735- S48P4XE-V2/ S5735- S48S4XE-V2/ S5735- S48U4XE-V2/ S5735- S48U4XE-V2/ S5735- S48U4XE-V2/ S5735- L10T4X- A-V2/ S5735- L14P2S- QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2X- QA-V2/

特性	特性限制	系列	涉及产品
特性	特性限制	系列	S5735- L16T4X- QA-V2/ S5735- L24P4S- A-V2/ S5735- L24P4XE- A-V2/ S5735- L24ST4XE -A-V2/ S5735- L24T4S- A-V2/ S5735- L24T4X- QA-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- A-V2/
			A-V2/ S5735- L48LP4XE -A-V2/ S5735- L48P4XE- A-V2/ S5735- L48S4X- A-V2/ S5735- L48T4S- A-V2/ S5735- L48T4XE- D-V2/ S5735- L48T4XE- D-V2/ S5735- L48T4XE- D-V2/ S5735- L48T4XE- D-V2/ S5735- L8P2T4X-

特性	特性限制	系列	涉及产品
特性	特性限制	系列	A-V2/ S5735- L8P4S-A- V2/ S5735- L8P4X- QA-V2/ S5735- L8T4S-A- V2/ S5735- L8T4X- QA-V2 S5735I- L10T4X- A-V2/ S5735I- L8P4X-A- V2 S5755- H24N4Y- A/S5755- H24P4Y2 CZ/ S5755- H24UAY2 CZ/ S5755- H24UN4Y 2CZ/ S5755- H24UN4Y 2CZ/ S5755- H24UN4Y 2CZ/ S5755- H24UN4Y 2CZ/ S5755- H24UN4Y 2CZ/ S5755- H24UN4Y 2CZ/ S5755- H24UN4Y 2CZ/ S5755- H24UN4Y 2CZ/ S5755- H24UN4Y 2CZ/ S5755- H24UN4Y 2CZ/ S5755- H24UN4Y 2CZ/ S5755- H24UN4Y 2CZ/ S5755- H24UN4Y 2CZ/ S5755- H24UN4Y 2CZ/ S5755- H24UN4Y 2CZ/ S5755- H48N4Y- A/S5755- H48P4Y2 CZ/ S5755- H48T4Y2 CZ/ S5755- H48T4Y2 CZ/ S5755-
			H48U4Y2 CZ/ S5755- H48UN4Y 2CZ/

特性	特性限制	系列	涉及产品
			S5755- H48UTM 4X4Y2C
			S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730- H48Y6C- V2
			S5732- H24S4X6 QZ-V2/ S5732- H24UM4 Y2CZ- KV2/ S5732- H24UM4 Y2CZ-V2/ S5732- H44S4X6 QZ-V2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/
			S5735I- S24T4XE- V2/ S5735I- S24U4XE- V2/ S5735I- S8T4SN- V2/ S5735I- S8T4XN- V2/

特性	特性限制	系列	涉及产品
			S5735I- S8U4XN- V2
			S5735I- H8T4S2X N-V2

# 3.4 配置流分类

# 前提条件

在配置流分类之前,需要完成以下任务:

如果使用ACL作为流分类规则,配置相应的ACL。

# 背景信息

流分类各规则之间属于并列关系,只要匹配规则不冲突,都可以在同一流分类中配置。用户使用时,请根据需要进行配置。

#### □ 说明

- 不支持在and模式流分类中同时匹配重复规则,如配置if-match source-mac,同时匹配包含 source-mac的ACL。
- 当在某一视图下,需要同时匹配同一类报文(如二层报文、IPv4报文、IPv6报文等)的多个字段时,请在该视图下应用1个流策略,并在该流策略中指定多个流分类及其所需的流行为。若需要同时匹配IPv4报文和IPv6报文,请为这两类报文分别创建1个流策略。

#### 操作步骤

步骤1 进入系统视图。

system-view

步骤2 创建一个流分类并进入流分类视图,或进入已存在的流分类视图。

traffic classifier classifier-name [ type { and | or } ]

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"。

步骤3 请根据实际情况定义流分类中的匹配规则。

#### □ 说明

各匹配规则的注意事项,请参见对应命令的命令参考。

# • 链路层规则(二层规则)

匹配规则	命令
目的MAC地址	<b>if-match destination-mac</b> <i>mac-address</i> [ <i>mac-address-mask</i> ]
源MAC地址	<b>if-match source-mac</b> <i>mac-address</i> [ <i>mac-address-mask</i> ]
以太网帧头中协议类 型字段	if-match l2-protocol { arp   ip   profinet   rarp   protocol-value }
VLAN报文外层Tag的 VLAN ID或QinQ报文 内外两层Tag的VLAN ID	if-match vlan start-vlan-value [ inner-vlan start-inner-vlan-value [ to end-inner-vlan-value ] ] if-match vlan start-vlan-value [ to end-vlan-value ] [ inner-vlan start-inner-vlan-value ]
VLAN报文外层Tag的 802.1p值	if-match 8021p 8021p-value &<1-8>
QinQ报文内层Tag的 VLAN ID	<b>if-match inner-vlan</b> <i>start-inner-vlan-value</i> [ <b>to</b> <i>end-inner-vlan-value</i> ]
QinQ报文内层Tag的 802.1p值	if-match inner-8021p inner-8021p-value &<1-8>
QinQ报文双层Tag的 VLAN ID	if-match double-tag

# • 网络层规则(三层规则)

匹配规则	命令
IP报文的DSCP优先级	if-match dscp dscp-value &<1-8>
IPv6报文的DSCP优先 级	if-match ipv6 dscp dscp-value &<1-8>
IP报文的IP优先级	if-match ip-precedence ip-precedence &<1-8>
IP报文的ECN拥塞标 记	if-match ecn ecn-value
IPv6报文的ECN拥塞 标记	if-match ipv6 ecn ecn-value

# • 传输层规则(四层规则)

匹配规则	命令
TCP报文头中的TCP Flag	if-match tcp-flag { tcp-flag-value   { ack   fin   psh   rst   syn   urg } * }

### ACL规则

匹配规则	命令
ACL规则	if-match acl { acl-number   acl-name }
ACL6规则	if-match ipv6 acl { acl-number   acl6-name } [ loose-mode   strict-mode ]
	<b>loose-mode</b> 和 <b>strict-mode</b> 参数仅S6730-H-V2、 S5732-H-V2和S5755-H系列支持。

#### • 转发规则

匹配规则	命令
丢弃报文	if-match discard
所有报文	if-match any
入接口	<pre>if-match inbound-interface { { interface-type interface-number1   interface-name1 } [ to { interface-type interface-number2   interface- name2 } ] } &amp;&lt;1-8&gt;</pre>
出接口	<pre>if-match outbound-interface { { interface-type interface-number1   interface-name1 } [ to { interface-type interface-number2   interface- name2 } ] } &amp;&lt;1-8&gt;</pre>
已知单播报文	if-match unicast
未知单播报文	if-match unknown-unicast

### ● VXLAN报文规则

匹配规则	命令
基于IPv4 ACL匹配 VXLAN内层报文	<pre>if-match vxlan [ transit ] acl { acl-number   acl- name }</pre>
基于IPv6 ACL匹配 VXLAN内层报文	if-match vxlan [ transit ] ipv6 acl { acl-number   acl-name } [ loose-mode   strict-mode ]
VXLAN内层报文信息	if-match vxlan [ transit ] vni vni-id

仅S6730-H-V2、S5732-H-V2和S5755-H系列支持VXLAN报文规则的命令。

## ● SRv6报文规则

匹配规则	命令
基于IPv4 ACL匹配 SRv6内层报文	<pre>if-match srv6 transit acl { acl-number   acl-name }</pre>

匹配规则	命令
基于IPv6 ACL匹配 SRv6内层报文	if-match srv6 transit ipv6 acl { acl-number   acl-name } [ loose-mode   strict-mode ]

仅S6730-H-V2、S5732-H-V2和S5755-H系列支持SRv6报文规则的命令。

#### • 其他规则

匹配规则	命令
QoS本地ID	if-match qos-local-id qos-local-id
MPLS报文的EXP优先 级	if-match mpls-exp <i>mpls-exp-value</i> &<1-8> 该功能仅S6730-H-V2、S5732-H-V2和S5755-H系列支 持。

步骤4 退出流分类视图。

quit

步骤5 (可选)开启修改MQC流分类规则时流量不中断功能。

traffic-policy atomic-update-mode

在配置此命令之后,如果修改流分类规则,则系统对于老的规则采取先下发后删除的方式,保证流量不会中断。

对于开启此功能后应用成功的流策略,如果因为配置变更导致应用失败,该流策略不会删除,仍然保持为原先应用成功的流策略。

缺省情况下,此功能关闭。

----结束

# 3.5 配置流行为

# 操作步骤

步骤1 进入系统视图。

system-view

步骤2 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。

traffic behavior behavior-name

**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。

# 山 说明

各动作的注意事项,请参见对应命令的命令参考。

动作	命令
配置报文过滤	参见 <b>4 报文过滤配置</b>

动作	命令
配置流量统计	参见5 流量统计配置
配置MQC实现重 标记	参见6 报文重标记配置
配置MQC实现重 定向	参见7 报文重定向配置
配置MQC实现流 量监管	参见 <b>流量监管、流量整形和接口限速配置</b> 中的 <b>9.7.1 配置一级</b> CAR的流量监管(MQC方式)
配置层次化流量 监管	car car-name share         参见流量监管、流量整形和接口限速配置中的9.7.2 配置二级         CAR的流量监管         仅S6730-H-V2、S5732-H-V2和S5755-H系列支持该功能。
配置MQC实现流 镜像	mirroring observe-port observe-port-index mirroring observe-port group group-id 详细功能请参见《CLI配置指南-系统监控配置》-"镜像配置"中的"配置流镜像"。
配置MQC实现禁 止MAC地址学习	mac-address learning disable 详细功能请参见《CLI配置指南-以太网交换配置》-"MAC配置"中的"关闭MAC地址学习功能"。
配置基于MQC实 现VLAN Mapping	vlan-mapping { vlan vlan-id   inner-vlan inner-vlan-id } 详细功能请参见《 CLI配置指南-以太网交换配置 》 - "VLAN配 置"中的"配置VLAN Mapping"。
配置基于MQC的 灵活QinQ	vlan-stacking vlan <i>vlan-id</i> 详细功能请参见《CLI配置指南-以太网交换配置》-"VLAN配置"中的"配置QinQ"。
去使能URPF检查	<b>ip urpf disable</b> 详细功能请参见《CLI配置指南-安全配置》中的"URPF配置"。 仅S6730-H-V2、S5732-H-V2和S5755-H系列支持该功能。
指定网络切片实 例	network-slice-instance netsliceinstid 详细功能请参见《CLI配置指南-网络切片配置》中的"网络切片 配置"。

----结束

# 3.6 配置流策略

# 前提条件

在配置流策略之前,需要完成以下任务:

- 配置流分类
- 配置流行为

# 操作步骤

步骤1 进入系统视图。

system-view

步骤2 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。

traffic policy policy-name

步骤3 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。

classifier classifier-name behavior behavior-name [ precedence precedence-value ]

----结束

# 3.7 应用流策略

# 前提条件

在应用流策略之前,请完成配置流策略。

#### □ 说明

如果流策略因设备上ACL资源不足而应用失败,建议删除应用失败的流策略配置。否则设备保存 配置并且重启后,其他已正常运行的业务的配置会恢复失败。

# 操作步骤

步骤1 进入系统视图。

system-view

步骤2 应用流策略。

- 在全局上应用流策略。
  - a. 在全局上应用流策略。 traffic-policy *policy-name* global [ slot *slot-id* ] { inbound | outbound }
- 在接口上应用流策略。
  - a. 进入接口视图。

interface interface-type interface-number

- b. 在接口上应用流策略。 traffic-policy *policy-name* { inbound | outbound }
- c. 退出接口视图。 quit
- 在VLAN上应用流策略。
  - a. 创建VLAN,并进入VLAN视图。 vlan vlan-id
  - b. 在VLAN上应用流策略。

traffic-policy policy-name { inbound | outbound }

应用后,系统对属于该VLAN并匹配流分类中规则的入方向或出方向报文实施 策略控制。 c. 退出VLAN视图。 quit

----结束

# 3.8 检查配置结果

# 操作步骤

操作	命令
查看已配置的流分类信息	display traffic classifier [ classifier- name ]
查看已配置的流行为信息	display traffic behavior [ behavior- name ]
查看已配置的流策略信息	display traffic policy [ policy-name [ classifier classifier-name ] ]
查看流策略的应用记录	display traffic-policy applied-record [ policy-name ]
查看TCAM下发失败的信息	display system tcam fail-record [ slot slot-id ]
查看不同的业务占用的组索引和规则计数	display system tcam service brief [ slot slot-id ]
	display system tcam service { cpcar slot slot-id   service-name slot slot-id [ chip chip-id ] }
查看流策略的应用数据	display system tcam service traffic- policy
查看规则命中的信息	display system tcam match-rules slot slot-id
查看应用流策略后的报文统计信息	display traffic-policy statistics
查看各视图下应用流策略时支持的匹配字 段和动作	display system tcam acl group- information
查看待应用的流策略所占用的资源信息, 以确认配置提交后对应的流策略是否能应 用成功	display traffic-policy pre-state

查询命令的详细功能请参见《命令参考》。

# 3.9 维护 MQC

# 背景信息

当需要对流策略的统计信息重新进行统计时,可以执行以下命令,清除之前的流策略 统计信息。

## 须知

清除流策略统计信息后,以前的统计信息将无法恢复,请于清除之前仔细确认。

# 操作步骤

• 清除应用流策略的统计信息。

reset traffic-policy statistics { global [ slot slot-id] | interface { interface-type interface-number | interface-name } | vlan vlan-id | vpn-instance vpn-instance-name } [ policy-name ] [ inbound | outbound ] [ classifier-base classifier-name ] [ history ]

#### □ 说明

**vpn-instance**参数仅S6730-H-V2、S5732-H-V2和S5755-H系列支持。

## ----结束

# **上**报文过滤配置

- 4.1 报文过滤简介
- 4.2 报文过滤配置注意事项
- 4.3 配置基于MQC的报文过滤
- 4.4 举例:配置基于MQC的报文过滤
- 4.5 举例:配置基于源MAC地址控制访问的示例

# 4.1 报文过滤简介

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

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

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。

# 4.2 报文过滤配置注意事项

# License 依赖

报文过滤无需License许可即可使用。

# 硬件依赖

表 4-1 支持本特性的硬件

系列	支持产品
S5735-L-V2 series	\$5735-L10T4X-A-V2/\$5735-L14P2S-QA-V2/\$5735-L16LP2UM2X-QA-V2/\$5735-L16LP2X-QA-V2/\$5735-L16P2UM2X-QA-V2/\$5735-L16T4S-A-V2/\$5735-L16T4X-QA-V2/\$5735-L24P4S-A-V2/\$5735-L24P4XE-A-V2/\$5735-L24ST4XE-A-V2/\$5735-L24T4S-A-V2/\$5735-L24T4XE-D-V2/\$5735-L24T4XE-A-V2/\$5735-L24T4XE-A-V2/\$5735-L48LP4S-A-V2/\$5735-L48LP4XE-A-V2/\$5735-L48P4XE-A-V2/\$5735-L48S4XE-A-V2/\$5735-L48S4XE-A-V2/\$5735-L48T4S-A-V2/\$5735-L48T4XE-A-V2/\$5735-L48T4XE-A-V2/\$5735-L48T4XE-A-V2/\$5735-L48T4XE-A-V2/\$5735-L48T4XE-A-V2/\$5735-L8P4X-QA-V2/\$5735-L8P4X-QA-V2/\$5735-L8P4X-QA-V2/\$5735-L8P4X-QA-V2/\$5735-L8P4X-QA-V2/\$5735-L8T4X-QA-V2
S5735-S-V2 series	S5735-S24HS4XE-V2/S5735-S24P4XE-V2/S5735- S24ST4XE-V2/S5735-S24T4XE-V2/S5735- S24U4XE-V2/S5735-S48HS4XE-V2/S5735- S48P4XE-V2/S5735-S48S4XE-V2/S5735-S48T4XE- V2/S5735-S48U4XE-V2
S5735I-L-V2 series	S5735I-L10T4X-A-V2/S5735I-L8P4X-A-V2
S5755-H series	S5755-H24N4Y-A/S5755-H24P4Y2CZ/S5755- H24T4Y2CZ/S5755-H24U4Y2CZ/S5755- H24UN4Y2CZ/S5755-H24UTM4X4Y2C/S5755- H48N4Y-A/S5755-H48P4Y2CZ/S5755-H48T4Y2CZ/ S5755-H48U4Y2CZ/S5755-H48UN4Y2CZ/S5755- H48UTM4X4Y2C
S6730-H-V2 series	S6730-H24X6C-V2/S6730-H28X6CZ-V2/S6730- H48X6C-V2/S6730-H48X6CZ-V2/S6730-H48Y6C- V2
S5732-H-V2 series	S5732-H24S4X6QZ-V2/S5732-H24UM4Y2CZ-KV2/ S5732-H24UM4Y2CZ-V2/S5732-H44S4X6QZ-V2/ S5732-H48UM4Y2CZ-KV2/S5732-H48UM4Y2CZ- V2
S5735I-H-V2 series	S5735I-H8T4S2XN-V2
S5735I-S-V2 series	S5735I-S24T4XE-V2/S5735I-S24U4XE-V2/S5735I- S8T4SN-V2/S5735I-S8T4XN-V2/S5735I-S8U4XN- V2

# 特性限制

无

# 4.3 配置基于 MQC 的报文过滤

# 背景信息

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

#### □ 说明

- 流行为中,permit动作与其他流动作一起配置时,将依次执行这些动作;deny动作与除流量统计、流镜像外的其他流动作互斥,即使配置其他流动作也不会生效。
- 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。
- MQC相关的配置注意事项,请参考MQC章节的配置注意事项页面。

# 操作步骤

#### 步骤1 配置流分类。

流分类的配置方式,请参考MQC配置中的3.4 配置流分类。

#### 步骤2 配置流行为。

- 1. 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。 traffic behavior behavior-name
- 2. 请根据实际需要配置如下流行为。
  - 配置流行为对匹配流分类规则的报文不做任何动作,按原来的策略转发。 permit

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。

- 配置流行为禁止匹配流分类规则的报文通过。

deny

流行为中,**deny**动作和其他流动作互斥,除流量统计和流镜像外,即使配置 其他动作也不会生效。

3. 退出流行为视图。

#### 步骤3 配置流策略。

- 1. 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。
  - traffic policy policy-name
- 2. 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。

classifier classifier-name behavior behavior-name [ precedence precedence-value ]

3. 退出流策略视图。

quit

#### 步骤4 应用流策略。

- 在全局上应用流策略。
  - a. 在全局上应用流策略。 traffic-policy *policy-name* global [ slot *slot-id* ] { inbound | outbound }

- 在接口上应用流策略。
  - a. 进入接口视图。

interface interface-type interface-number

- b. 在接口上应用流策略。 traffic-policy *policy-name* { inbound | outbound }
- c. 退出接口视图。 quit
- 在VLAN上应用流策略。
  - a. 创建VLAN,并进入VLAN视图。

vlan vlan-id

- b. 在VLAN上应用流策略。traffic-policy policy-name { inbound | outbound }应用后,系统对属于该VLAN并匹配流分类中规则的入方向或出方向报文实施策略控制。
- c. 退出VLAN视图。 quit

## ----结束

# 检查配置结果

操作	命令
查看已配置的流分类信息	display traffic classifier [ classifier- name ]
查看已配置的流行为信息	display traffic behavior [ behavior- name ]
查看已配置的流策略信息	display traffic policy [ policy-name [ classifier classifier-name ] ]
查看流策略的应用记录	display traffic-policy applied-record [ policy-name ]
查看TCAM下发失败的信息	display system tcam fail-record [ slot slot-id ]
查看不同的业务占用的组索引和规则计数	display system tcam service brief [ slot slot-id ]
	display system tcam service { cpcar slot slot-id   service-name slot slot-id [ chip chip-id ] }
查看流策略的应用数据	display system tcam service traffic- policy

操作	命令
查看规则命中的信息	display system tcam match-rules slot slot-id
查看应用流策略后的报文统计信息	display traffic-policy statistics
查看各视图下应用流策略时支持的匹配字 段和动作	display system tcam acl group- information
查看待应用的流策略所占用的资源信息, 以确认配置提交后对应的流策略是否能应 用成功	display traffic-policy pre-state

# 4.4 举例:配置基于 MQC 的报文过滤

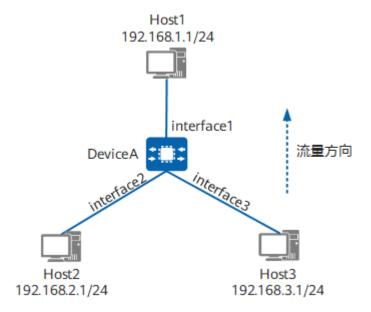
# 组网需求

如<mark>图4-1</mark>所示,Host1、2、3通过DeviceA实现互访。现要求Host1的用户可以通过DeviceA收到Host2发送的流量,但是不能收到Host3发送的流量。

## 图 4-1 配置报文过滤组网图

# □ 说明

本例中interface1, interface2, interface3分别代表10GE1/0/1, 10GE1/0/2和10GE1/0/3。



# 操作步骤

#### 步骤1 配置ACL规则

# 在DeviceA上创建ACL3001,匹配源IP为192.168.3.1且目的IP为192.168.1.1的流,即从Host3到Host1的流量。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] acl 3001
[DeviceA-acl4-advance-3001] rule permit ip destination 192.168.1.1 0.0.0.255 source 192.168.3.1
0.0.0.255
[DeviceA-acl4-advance-3001] quit
```

## 步骤2 配置流分类

# 在DeviceA上创建流分类c1,匹配规则为ACL3001。

```
[DeviceA] traffic classifier c1
[DeviceA-classifier-c1] if-match acl 3001
[DeviceA-classifier-c1] quit
```

## 步骤3 配置流行为

# 在DeviceA上创建流行为b1,并配置禁止动作。

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

## 步骤4 配置流策略并应用到接口10GE1/0/1的出方向上

# 在DeviceA上创建流策略p1,将流分类和对应的流行为进行绑定。

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

#将流策略p1应用到接口10GE1/0/1的出方向上。

```
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] traffic-policy p1 outbound
[DeviceA-10GE1/0/1] quit
[DeviceA] quit
```

#### ----结束

# 检查配置结果

#查看ACL规则的配置信息。

```
<DeviceA> display acl 3001
Advanced ACL 3001, 1 rule
ACL's step is 5
rule 5 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
(0 times matched)
```

# 查看流分类的配置信息。

```
<DeviceA> display traffic classifier c1
Traffic Classifier Information:
Classifier: c1
Type: OR
Rule(s):
if-match acl 3001
```

# 查看流策略的配置信息。

```
<DeviceA> display traffic policy p1
Traffic Policy Information:
Policy: p1
Classifier: c1
Type: OR
Behavior: b1
Deny
```

# 配置脚本

#### DeviceA的配置脚本

```
# sysname DeviceA
# acl number 3001
rule 5 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
# traffic classifier c1 type or if-match acl 3001
# traffic behavior b1
deny
# traffic policy p1
classifier c1 behavior b1 precedence 5
# interface 10GE1/0/1
traffic-policy p1 outbound
# return
```

# 4.5 举例: 配置基于源 MAC 地址控制访问的示例

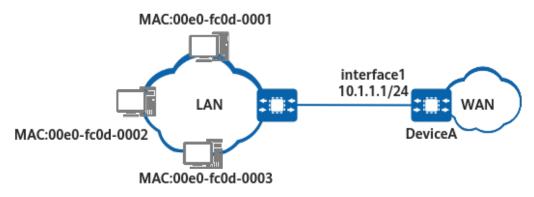
# 组网需求

如<mark>图4-2</mark>所示,企业内用户通过DeviceA访问互联网。现要求限制局域网内某些主机访问互联网,但是由于这些主机可以变换IP地址,所以通过防火墙限制不能有效防范,最合适的做法是基于源MAC地址进行限制。在本例中可以实现限制某些主机访问互联网,但是可以访问DeviceA。

## 图 4-2 配置组网图

## 山 说明

本例中interface1代表10GE1/0/1。



# 操作步骤

#### 步骤1 创建VLAN并配置接口。

# 在DeviceA上创建VLAN 10, 配置vlanif10, 并将接口10GE1/0/1加入VLAN。

<HUAWEI> system-view

[HUAWEI] sysname DeviceA

[DeviceA] vlan 10

[DeviceA-vlan10] quit

[DeviceA] interface 10ge 1/0/1

[DeviceA-10GE1/0/1] port link-type trunk

[DeviceA-10GE1/0/1] port trunk allow-pass vlan 10

[DeviceA-10GE1/0/1] quit

[DeviceA] interface vlanif 10

[DeviceA-Vlanif10] ip address 10.1.1.1 255.255.255.0

#### 步骤2 配置ACL规则

# 在DeviceA上创建ACL3001, 匹配目的IP为10.1.1.1/24的流。

[DeviceA] acl 3001

[DeviceA-acl4-advance-3001] rule 1 permit ip destination 10.1.1.0 0.0.0.255

[DeviceA-acl4-advance-3001] quit

## 步骤3 配置流分类

#在DeviceA上创建流分类c1, 匹配规则为ACL3001。

[DeviceA] traffic classifier c1 type and

[DeviceA-classifier-c1] if-match acl 3001

[DeviceA-classifier-c1] quit

# 在DeviceA上创建流分类c2~c4, 匹配用户主机的MAC地址。

[DeviceA] traffic classifier c2 type and

[DeviceA-classifier-c2] if-match source-mac 00e0-fc0d-0001

[DeviceA-classifier-c2] quit

[DeviceA] traffic classifier c3 type and

[DeviceA-classifier-c3] **if-match source-mac 00e0-fc0d-0002** 

[DeviceA-classifier-c3] quit

[DeviceA] traffic classifier c4 type and

[DeviceA-classifier-c4] if-match source-mac 00e0-fc0d-0003

[DeviceA-classifier-c4] quit

#### 步骤4 配置流行为

# 在DeviceA上创建流行为b1,并配置允许动作。

[DeviceA] traffic behavior b1

[DeviceA-behavior-b1] permit

[DeviceA-behavior-b1] quit

# 在DeviceA上创建流行为b2,并配置禁止动作。

[DeviceA] traffic behavior b2

[DeviceA-behavior-b2] deny

[DeviceA-behavior-b2] quit

## 步骤5 配置流策略并应用到接口的入方向上

# 在DeviceA上创建流策略p1,将流分类和对应的流行为进行绑定。

[DeviceA] traffic policy p1

[DeviceA-trafficpolicy-p1] classifier c1 behavior b1 precedence 5

[DeviceA-trafficpolicy-p1] classifier c2 behavior b2 precedence 10

[DeviceA-trafficpolicy-p1] classifier c3 behavior b2 precedence 15

[DeviceA-trafficpolicy-p1] classifier c4 behavior b2 precedence 20

[DeviceA-trafficpolicy-p1] quit

## # 将流策略p1应用到接口的入方向上。

```
[DeviceA] interface vlanif 10
[DeviceA-Vlanif10] traffic-policy p1 inbound
[DeviceA-Vlanif10] quit
[DeviceA] quit
```

#### ----结束

# 检查配置结果

# #查看ACL规则的配置信息。

```
<DeviceA> display acl 3001
Advanced ACL 3001, 1 rule
ACL's step is 5
rule 1 permit ip destination 10.1.1.0 0.0.0.255
(0 times matched)
```

#### # 查看流分类的配置信息。

```
<DeviceA> display traffic classifier c1
Traffic Classifier Information:
   Classifier: c1
   Type: AND
   Rule(s):
     if-match acl 3001
<DeviceA> display traffic classifier c2
Traffic Classifier Information:
   Classifier: c2
   Type: AND
   Rule(s):
     if-match source-mac 00e0-fc0d-0001 ffff-ffff
```

#### # 查看流策略的配置信息。

```
<DeviceA> display traffic policy p1
 Traffic Policy Information:
  Policy: p1
   Classifier: c1
     Type: AND
    Behavior: b1
   Classifier: c2
     Type: AND
   Behavior: b2
     Deny
   Classifier: c3
     Type: AND
    Behavior: b2
     Deny
   Classifier: c4
    Type: AND
    Behavior: b2
    Deny
```

# 配置脚本

#### DeviceA的配置脚本

```
#
sysname DeviceA
#
vlan 10
#
interface 10ge 1/0/1
port link-type trunk
port trunk allow-pass vlan 10
```

```
interface vlanif 10
ip address 10.1.1.1 255.255.255.0
acl 3001
rule 1 permit ip destination 10.1.1.0 0.0.0.255
traffic classifier c1 type and
if-match acl 3001
traffic classifier c2 type and if-match source-mac 00e0-fc0d-0001
traffic classifier c3 type and if-match source-mac 00e0-fc0d-0002
traffic classifier c4 type and
if-match source-mac 00e0-fc0d-0003
traffic behavior b1
permit
traffic behavior b2
deny
traffic policy p1
classifier c1 behavior b1 precedence 5
classifier c2 behavior b2 precedence 10
classifier c3 behavior b2 precedence 15
classifier c4 behavior b2 precedence 20
interface vlanif 10
traffic-policy p1 inbound
return
```

# **5** 流量统计配置

- 5.1 流量统计简介
- 5.2 流量统计配置注意事项
- 5.3 配置基于MQC的流量统计
- 5.4 举例: 配置基于MQC的流量统计

# 5.1 流量统计简介

流量统计支持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5-1所示。

表 5-1 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

# 5.2 流量统计配置注意事项

# License 依赖

流量统计无需License许可即可使用。

# 硬件依赖

表 5-2 支持本特性的硬件

系列	支持产品
S5735-L-V2 series	S5735-L10T4X-A-V2/S5735-L14P2S-QA-V2/S5735-L16LP2UM2X-QA-V2/S5735-L16LP2X-QA-V2/S5735-L16P2UM2X-QA-V2/S5735-L16T4S-A-V2/S5735-L16T4X-QA-V2/S5735-L24P4S-A-V2/S5735-L24P4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L48LP4S-A-V2/S5735-L48LP4XE-A-V2/S5735-L48P4XE-A-V2/S5735-L48S4XE-A-V2/S5735-L48T4S-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L8P4X-A-V2/S5735-L8P4X-A-V2/S5735-L8P4X-A-V2/S5735-L8P4X-QA-V2/S5735-L8P4X-QA-V2/S5735-L8P4X-QA-V2/S5735-L8P4X-QA-V2/S5735-L8T4X-QA-V2
S5735-S-V2 series	S5735-S24HS4XE-V2/S5735-S24P4XE-V2/S5735- S24ST4XE-V2/S5735-S24T4XE-V2/S5735- S24U4XE-V2/S5735-S48HS4XE-V2/S5735- S48P4XE-V2/S5735-S48S4XE-V2/S5735-S48T4XE- V2/S5735-S48U4XE-V2
S5735I-L-V2 series	S5735I-L10T4X-A-V2/S5735I-L8P4X-A-V2
S5755-H series	S5755-H24N4Y-A/S5755-H24P4Y2CZ/S5755- H24T4Y2CZ/S5755-H24U4Y2CZ/S5755- H24UN4Y2CZ/S5755-H24UTM4X4Y2C/S5755- H48N4Y-A/S5755-H48P4Y2CZ/S5755-H48T4Y2CZ/ S5755-H48U4Y2CZ/S5755-H48UN4Y2CZ/S5755- H48UTM4X4Y2C
S6730-H-V2 series	S6730-H24X6C-V2/S6730-H28X6CZ-V2/S6730- H48X6C-V2/S6730-H48X6CZ-V2/S6730-H48Y6C- V2
S5732-H-V2 series	S5732-H24S4X6QZ-V2/S5732-H24UM4Y2CZ-KV2/ S5732-H24UM4Y2CZ-V2/S5732-H44S4X6QZ-V2/ S5732-H48UM4Y2CZ-KV2/S5732-H48UM4Y2CZ- V2
S5735I-H-V2 series	S5735I-H8T4S2XN-V2
S5735I-S-V2 series	S5735I-S24T4XE-V2/S5735I-S24U4XE-V2/S5735I- S8T4SN-V2/S5735I-S8T4XN-V2/S5735I-S8U4XN- V2

# 特性限制

无

# 5.3 配置基于 MQC 的流量统计

# 背景信息

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

#### □ 说明

- 当流策略中配置的规则比较多的情况下,如果先清除了统计信息,再查看流量统计,可能会 出现统计信息显示为空或者只显示部分统计信息的情况,请等待一段时间再进行统计信息的 查看。
- 包含较多规则的流策略定义流量统计动作,基于实例或流分类去查询统计计数常会出现命令 行执行卡顿的现象。
- MQC相关的配置注意事项,请参考MQC章节的配置注意事项页面。

# 操作步骤

#### 步骤1 配置流分类。

流分类的配置方式,请参考MQC配置中的3.4 配置流分类。

#### 步骤2 配置流行为。

(可选)配置流量统计时包括以太网帧的帧间隙和前导码。

qos statistics ifg enable

2. 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。

traffic behavior behavior-name

3. 使能流量统计功能。

statistics enable [ history-record interval interval-value ]

4. 退出流行为视图。

quit

#### 步骤3 配置流策略。

1. 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。

traffic policy policy-name

2. 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。

classifier classifier-name behavior behavior-name [ precedence precedence-value ]

3. 退出流策略视图。

quit

#### 步骤4 应用流策略。

- 在全局上应用流策略。
  - a. 在全局上应用流策略。 traffic-policy *policy-name* global [ slot *slot-id* ] { inbound | outbound }
- 在接口上应用流策略。
  - a. 进入接口视图。

interface interface-type interface-number

- b. 在接口上应用流策略。 traffic-policy policy-name { inbound | outbound }
- c. 退出接口视图。 quit
- 在VLAN上应用流策略。
  - a. 创建VLAN,并进入VLAN视图。 vlan vlan-id

  - c. 退出VLAN视图。 quit

## ----结束

# 检查配置结果

操作	命令
查看已配置的流分类信息	display traffic classifier [ classifier- name ]
查看已配置的流行为信息	display traffic behavior [ behavior- name ]
查看已配置的流策略信息	display traffic policy [ policy-name [ classifier classifier-name ] ]
查看流策略的应用记录	display traffic-policy applied-record [ policy-name ]
查看TCAM下发失败的信息	display system tcam fail-record [ slot slot-id ]
查看不同的业务占用的组索引和规则计数	display system tcam service brief [ slot slot-id ]
	display system tcam service { cpcar slot slot-id   service-name slot slot-id [ chip chip-id ] }
查看流策略的应用数据	display system tcam service traffic- policy
查看规则命中的信息	display system tcam match-rules slot slot-id

操作	命令
查看应用流策略后的报文统计信息	display traffic-policy statistics
查看各视图下应用流策略时支持的匹配字 段和动作	display system tcam acl group- information
查看待应用的流策略所占用的资源信息, 以确认配置提交后对应的流策略是否能应 用成功	display traffic-policy pre-state

# 5.4 举例: 配置基于 MQC 的流量统计

# 组网需求

如<mark>图5-1</mark>所示,Host1发往DeviceA的报文中,业务报文的802.1p优先级为6。现在对业务报文进行流量统计,以确定带宽资源的分配。

#### 图 5-1 配置流量统计组网图

#### □ 说明

本例中interface1代表10GE1/0/1。



# 操作步骤

## 步骤1 配置ACL规则

#在DeviceA上创建编码为4000的二层ACL,匹配802.1p值为6的报文。

[DeviceA] acl 4000 [DeviceA-acl-L2-4000] rule permit 8021p 6 [DeviceA-acl-L2-4000] quit

## 步骤2 配置流分类

# 在DeviceA上创建流分类c1,匹配规则为ACL4000。

[DeviceA] traffic classifier c1 [DeviceA-classifier-c1] if-match acl 4000 [DeviceA-classifier-c1] quit

# 步骤3 配置流行为

# 在DeviceA上创建流行为b1,并配置流量统计动作。

[DeviceA] **traffic behavior b1** [DeviceA-behavior-b1] **statistics enable** [DeviceA-behavior-b1] **quit** 

## 步骤4 配置流策略并应用到接口上

#在DeviceA上创建流策略p1,将流分类和对应的流行为进行绑定。

[DeviceA] **traffic policy p1**[DeviceA-trafficpolicy-p1] **classifier c1 behavior b1**[DeviceA-trafficpolicy-p1] **quit** 

#将流策略p1应用到接口10GE1/0/1的入方向上。

[DeviceA] interface 10ge 1/0/1 [DeviceA-10GE1/0/1] traffic-policy p1 inbound [DeviceA-10GE1/0/1] quit [DeviceA] quit

----结束

# 检查配置结果

#查看ACL规则的配置信息。

<DeviceA> display acl 4000 L2 ACL 4000, 1 rule ACL's step is 5 rule 5 permit 8021p 6 (0 times matched)

# 查看流分类的配置信息。

#### <DeviceA> display traffic classifier c1 Traffic Classifier Information: Classifier: c1 Type: OR Rule(s): if-match acl 4000

# 查看流策略的配置信息。

<DeviceA> display traffic policy p1
Traffic Policy Information:
Policy: p1
Classifier: c1
Type: OR
Behavior: b1
Statistics: enable

#### # 查看流量统计信息。

# <DeviceA> display traffic-policy statistics interface 10ge 1/0/1 inbound Traffic policy: p1, inbound

Slot: 1 Item	Packets	Bytes	pp	os t	ops
Matched Passed Dropped Filter CAR	212185 212185 0 0 0	220674 2206744 0 0 0		1600 1600 0 0	1379215 1379215

可以看到接口10GE1/0/1下业务报文的流量统计信息。

# 配置脚本

# DeviceA的配置脚本

```
# sysname DeviceA
# vlan batch 100
# acl number 4000
rule 5 permit 8021p 6
# traffic classifier c1 type or
if-match acl 4000
# traffic behavior b1
statistics enable
# traffic policy p1
classifier c1 behavior b1 precedence 5
# interface 10GE1/0/1
traffic-policy p1 inbound
# return
```

# 6 报文重标记配置

- 6.1 报文重标记简介
- 6.2 报文重标记原理
- 6.3 报文重标记配置注意事项
- 6.4 配置基于MQC的报文重标记
- 6.5 举例:配置基于MQC的报文重标记

# 6.1 报文重标记简介

重标记是将报文的某个字段(如优先级)进行重新设置,使报文根据重标记后的信息进行调度或转发。例如,将符合某类规则的报文重新设置优先级,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,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。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,报文将在后续的转发中根据新设置的802.1p值进行调度和转发。

# 6.2 报文重标记原理

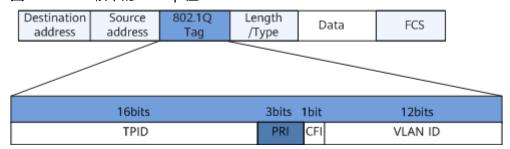
# 报文优先级字段

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:

## ● VLAN帧头中的802.1p值

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值),或称CoS(Class of Service)字段,标识了服务质量需求。VLAN帧中的802.1p值位置如图6-1所示。



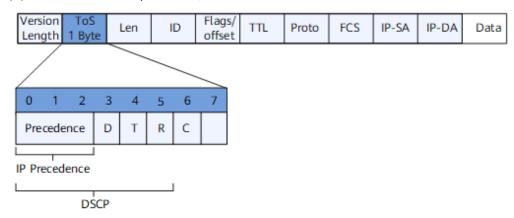


在802.1Q头部中包含3比特长的PRI字段和1比特长的CFI字段。PRI字段定义了8种业务优先级CoS,按照优先级从高到低顺序取值为7、6、5、4、3、2、1和0。CFI字段可以用来标识报文的丢弃优先级。

#### • IP报文中的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<mark>图 6-2</mark>所示。

图 6-2 IP Precedence/DSCP 字段



比特0~2表示Precedence字段,代表报文传输的8个优先级,按照优先级从高到低顺序取值为7、6、5、4、3、2、1和0。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Precedence字段外,ToS域中还包括D、T、R三个比特:

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

#### ● IP报文中的DSCP值

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6-2所示。

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

# 报文重标记

报文重标记是将上述和QoS相关的报文字段进行设置,重新定义报文的调度和传输方式。目前设备支持下面几种报文重标记的方式。

- 重标记VLAN报文中的802.1p值
- 重标记IP报文中的DSCP值
- 重标记报文的设备内部优先级
- 重标记QoS本地ID

# 6.3 报文重标记配置注意事项

# License 依赖

报文重标记无需License许可即可使用。

# 硬件依赖

表 6-1 支持本特性的硬件

系列	支持产品
S5735-L-V2 series	S5735-L10T4X-A-V2/S5735-L14P2S-QA-V2/S5735-L16LP2UM2X-QA-V2/S5735-L16LP2X-QA-V2/S5735-L16LP2UM2X-QA-V2/S5735-L16T4S-A-V2/S5735-L16T4X-QA-V2/S5735-L24P4X-A-V2/S5735-L24P4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L48LP4S-A-V2/S5735-L48LP4XE-A-V2/S5735-L48P4XE-A-V2/S5735-L48S4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L8P4X-A-V2/S5735-L8P4X-A-V2/S5735-L8P4X-A-V2/S5735-L8P4X-QA-V2/S5735-L8T4X-QA-V2
S5735-S-V2 series	S5735-S24HS4XE-V2/S5735-S24P4XE-V2/S5735- S24ST4XE-V2/S5735-S24T4XE-V2/S5735- S24U4XE-V2/S5735-S48HS4XE-V2/S5735- S48P4XE-V2/S5735-S48S4XE-V2/S5735-S48T4XE- V2/S5735-S48U4XE-V2
S5735I-L-V2 series	S5735I-L10T4X-A-V2/S5735I-L8P4X-A-V2
S5755-H series	S5755-H24N4Y-A/S5755-H24P4Y2CZ/S5755- H24T4Y2CZ/S5755-H24U4Y2CZ/S5755- H24UN4Y2CZ/S5755-H24UTM4X4Y2C/S5755- H48N4Y-A/S5755-H48P4Y2CZ/S5755-H48T4Y2CZ/ S5755-H48U4Y2CZ/S5755-H48UN4Y2CZ/S5755- H48UTM4X4Y2C

系列	支持产品
S6730-H-V2 series	S6730-H24X6C-V2/S6730-H28X6CZ-V2/S6730- H48X6C-V2/S6730-H48X6CZ-V2/S6730-H48Y6C- V2
S5732-H-V2 series	S5732-H24S4X6QZ-V2/S5732-H24UM4Y2CZ-KV2/ S5732-H24UM4Y2CZ-V2/S5732-H44S4X6QZ-V2/ S5732-H48UM4Y2CZ-KV2/S5732-H48UM4Y2CZ- V2
S5735I-H-V2 series	S5735I-H8T4S2XN-V2
S5735I-S-V2 series	S5735I-S24T4XE-V2/S5735I-S24U4XE-V2/S5735I- S8T4SN-V2/S5735I-S8T4XN-V2/S5735I-S8U4XN- V2

# 特性限制

表 6-2 本特性的使用限制

特性限制	系列	涉及产品
		L48T4XE-A-V2/ S5735-L48T4XE- D-V2/S5735- L8P2T4X-A-V2/ S5735-L8P4S-A- V2/S5735-L8P4X- QA-V2/S5735- L8T4S-A-V2/ S5735-L8T4X-QA- V2
		S5735I-L10T4X-A- V2/S5735I-L8P4X- A-V2
		S5755-H24N4Y-A/ S5755- H24P4Y2CZ/ S5755- H24T4Y2CZ/ S5755- H24UAY2CZ/ S5755- H24UN4Y2CZ/ S5755- H24UTM4X4Y2C/ S5755- H48P4Y2CZ/ S5755- H48T4Y2CZ/ S5755- H48U4Y2CZ/ S5755- H48U4Y2CZ/ S5755- H48U4Y2CZ/ S5755- H48UAY2CZ/ S5755- H48UAY2CZ/ S5755- H48UAY2CZ/ S5755- H48UAY2CZ/ S5755- H48UAY2CZ/ S5755- H48UAY2CZ/ S5755- H48UAY2CZ/ S5755- H48UAY2CZ/ S5755- H48UAY2CZ/ S6730-H24X6C- V2/S6730- H28X6CZ-V2/ S6730-H48X6C- V2/S6730- H48X6CZ-V2/
		S6730-H48Y6C-V2 S5732-
		H24S4X6QZ-V2/ S5732- H24UM4Y2CZ- KV2/S5732- H24UM4Y2CZ-V2/ S5732-

特性限制	系列	涉及产品
		H44S4X6QZ-V2/ S5732- H48UM4Y2CZ- KV2/S5732- H48UM4Y2CZ-V2
		S5735I-S24T4XE- V2/S5735I- S24U4XE-V2/ S5735I-S8T4SN- V2/S5735I- S8T4XN-V2/ S5735I-S8U4XN- V2 S5735I- H8T4S2XN-V2

特性限制	系列	涉及产品
基于MQC Remark本地优先级的约束: - 仅支持入方向应用。	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S5755-H series S6730-H-V2 series S5732-H-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735-S24HS4XE-V2/S5735-S24P4XE-V2/S5735-S24ST4XE-V2/S5735-S24T4XE-V2/S5735-S24U4XE-V2/S5735-S48HS4XE-V2/S5735-S48S4XE-V2/S5735-S48U4XE-S4-V2/S5735-S48U4XE-S4-V2/S5735-S48U4XE-S4-V2/S5735-S48U4XE-S4-V2/S5735-S48U4XE-S4-V2/S5735-S48U4XE-S4-V2/S5735-S48U4XE-S4-V2/S5735-S5-S5-S5-S5-S5-S5-S5-S5-S5-S5-S5-S5-S5

特性限制	系列	涉及产品
		S5735-L8P4S-A- V2/S5735-L8P4X- QA-V2/S5735- L8T4S-A-V2/ S5735-L8T4X-QA- V2
		S5735I-L10T4X-A- V2/S5735I-L8P4X- A-V2
		A-V2 S5755-H24N4Y-A/ S5755- H24P4Y2CZ/ S5755- H24U4Y2CZ/ S5755- H24UN4Y2CZ/ S5755- H24UTM4X4Y2C/ S5755- H24UTM4X4Y2C/ S5755- H48P4Y2CZ/ S5755- H48T4Y2CZ/ S5755- H48UN4Y2CZ/ S5755-
		V2/S6730- H28X6CZ-V2/ S6730-H48X6C- V2/S6730- H48X6CZ-V2/ S6730-H48Y6C-V2
		S5732- H24S4X6QZ-V2/ S5732- H24UM4Y2CZ- KV2/S5732- H24UM4Y2CZ-V2/ S5732- H44S4X6QZ-V2/ S5732-
		H48UM4Y2CZ-

特性限制	系列	涉及产品
		KV2/S5732- H48UM4Y2CZ-V2
		S5735I-S24T4XE- V2/S5735I- S24U4XE-V2/ S5735I-S8T4SN- V2/S5735I- S8T4XN-V2/ S5735I-S8U4XN- V2
		S5735I- H8T4S2XN-V2

# 6.4 配置基于 MQC 的报文重标记

# 背景信息

配置重标记后,设备将对符合流分类规则的报文重标记,使报文根据重标记后的信息进行调度或转发。

## 山 说明

- 支持在同一个流策略中同时配置remark 8021p和remark dscp的流行为,并同时生效。
- MQC相关的配置注意事项,请参考MQC章节的配置注意事项页面。

# 操作步骤

步骤1 配置流分类。

流分类的配置方式,请参考MQC配置中的3.4 配置流分类。

## 步骤2 配置流行为。

- 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。 traffic behavior behavior-name
- 2. 请根据实际需要配置如下流行为。
  - 重标记VLAN报文802.1p优先级 对于S6730-H-V2、S5732-H-V2和S5755-H系列:

remark 8021p { 8021p-value | inner-8021p }

对于S5735-L-V2、S5735-S-V2、S5735I-L-V2、S5735I-S-V2、S5735I-H-V2 系列:

remark 8021p 8021p-value

- 重标记IP报文的DSCP优先级
  - remark dscp { dscp-name | dscp-value }
- 重标记内部优先级

remark local-precedence { local-precedence-name | local-precedence-value } [ color ]

- 重标记QoS本地ID

对于S6730-H-V2系列:

remark qos-local-id [ inbound-match ]

对于S5735-L-V2、S5735-S-V2、S5735I-L-V2、S5735I-S-V2、S5755-H、S5732-H-V2、S5735I-H-V2系列:

remark qos-local-id qos-local-id inbound-match

3. 退出流行为视图。

#### 步骤3 配置流策略。

1. 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。

traffic policy policy-name

2. 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。

classifier classifier-name behavior behavior-name [ precedence precedence-value ]

3. 退出流策略视图。

quit

#### 步骤4 应用流策略。

- 在全局上应用流策略。
  - a. 在全局上应用流策略。 traffic-policy policy-name global [ slot slot-id ] { inbound | outbound }
- 在接口上应用流策略。
  - a. 进入接口视图。

interface interface-type interface-number

b. 在接口上应用流策略。 traffic-policy *policy-name* { inbound | outbound }

c. 退出接口视图。 quit

- 在VLAN上应用流策略。
  - a. 创建VLAN,并进入VLAN视图。

vlan vlan-id

b. 在VLAN上应用流策略。

traffic-policy policy-name { inbound | outbound }

应用后,系统对属于该VLAN并匹配流分类中规则的入方向或出方向报文实施 策略控制。

c. 退出VLAN视图。 quit

----结束

# 检查配置结果

操作	命令
查看已配置的流分类信息	display traffic classifier [ classifier- name ]

操作	命令
查看已配置的流行为信息	display traffic behavior [ behavior- name ]
查看已配置的流策略信息	display traffic policy [ policy-name [ classifier classifier-name ] ]
查看流策略的应用记录	display traffic-policy applied-record [ policy-name ]
查看TCAM下发失败的信息	display system tcam fail-record [ slot slot-id ]
查看不同的业务占用的组索引和规则计数	display system tcam service brief [ slot slot-id ]
	display system tcam service { cpcar slot slot-id   service-name slot slot-id [ chip chip-id ] }
查看流策略的应用数据	display system tcam service traffic- policy
查看规则命中的信息	display system tcam match-rules slot slot-id
查看应用流策略后的报文统计信息	display traffic-policy statistics
查看各视图下应用流策略时支持的匹配字 段和动作	display system tcam acl group- information
查看待应用的流策略所占用的资源信息, 以确认配置提交后对应的流策略是否能应 用成功	display traffic-policy pre-state

# 6.5 举例: 配置基于 MQC 的报文重标记

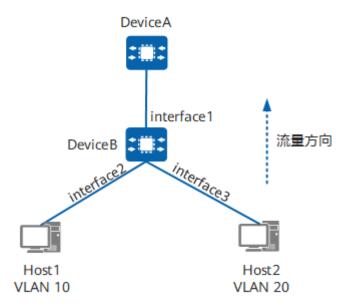
# 组网需求

如<mark>图6-3</mark>所示,Host1、Host2发往DeviceB的报文以不同的VLAN ID进行标识,Host1的VLAN ID为10,Host2的VLAN ID为20。DeviceB对从Host1和Host2收到的VLAN报文进行重标记,让Host1发出的报文在DeviceA中的设备内部优先级高于Host2发出的报文,从而保障Host1的业务体验。

#### 图 6-3 配置报文重标记组网图

#### 山 说明

本例中interface1, interface2, interface3分别代表10GE1/0/1, 10GE1/0/2和10GE1/0/3。



# 操作步骤

步骤1 创建VLAN并配置各接口,实现DeviceB与Host1、Host2、DeviceA互连。

# 在DeviceB上创建VLAN10、VLAN20和VLAN30。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] vlan batch 10 20 30
```

# 配置接口10GE1/0/1的接口类型为Trunk并加入VLAN30,10GE1/0/2、10GE1/0/3的接口类型为Access,分别加入VLAN10、VLAN20。

```
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] portswitch
[DeviceB-10GE1/0/1] port link-type trunk
[DeviceB-10GE1/0/1] port trunk allow-pass vlan 30
[DeviceB-10GE1/0/1] quit
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] portswitch
[DeviceB-10GE1/0/2] port link-type access
[DeviceB-10GE1/0/2] port default vlan 10
[DeviceB-10GE1/0/2] quit
[DeviceB] interface 10ge 1/0/3
[DeviceB-10GE1/0/3] portswitch
[DeviceB-10GE1/0/3] port link-type access
[DeviceB-10GE1/0/3] port default vlan 20
[DeviceB-10GE1/0/3] quit
```

# 创建VLANIF10、VLANIF20、VLANIF30,并为VLANIF接口配置IP地址。

```
[DeviceB] interface vlanif 10
[DeviceB-Vlanif10] ip address 192.168.10.1 24
[DeviceB-Vlanif10] quit
[DeviceB] interface vlanif 20
[DeviceB-Vlanif20] ip address 192.168.20.1 24
```

```
[DeviceB-Vlanif20] quit
[DeviceB] interface vlanif 30
[DeviceB-Vlanif30] ip address 192.168.100.1 24
[DeviceB-Vlanif30] quit
```

#### 步骤2 配置流分类

# 在DeviceB上创建并配置流分类c1、c2,对报文按照VLAN ID进行分类。

```
[DeviceB] traffic classifier c1
[DeviceB-classifier-c1] if-match vlan 10
[DeviceB-classifier-c1] quit
[DeviceB] traffic classifier c2
[DeviceB-classifier-c2] if-match vlan 20
[DeviceB-classifier-c2] quit
```

## 步骤3 配置流行为

# 在DeviceB上创建并配置流行为b1、b2,将Host1上送的VLAN报文的802.1p值重标记为4,Host2上送的报文重标记为2,实现Host1优先级高于Host2。

```
[DeviceB] traffic behavior b1
[DeviceB-behavior-b1] remark 8021p 4
[DeviceB-behavior-b1] quit
[DeviceB] traffic behavior b2
[DeviceB-behavior-b2] remark 8021p 2
[DeviceB-behavior-b2] quit
```

## 步骤4 配置流策略并应用到接口上

# 在DeviceB上创建流策略p1、p2,绑定流分类和对应的流行为,并将流策略p1应用 到接口10GE1/0/2入方向,将流策略p2应用到接口10GE1/0/3入方向,对报文进行重标 记。

```
[DeviceB] traffic policy p1
[DeviceB-trafficpolicy-p1] classifier c1 behavior b1
[DeviceB-trafficpolicy-p1] quit
[DeviceB] traffic policy p2
[DeviceB-trafficpolicy-p2] classifier c2 behavior b2
[DeviceB-trafficpolicy-p2] quit
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] traffic-policy p1 inbound
[DeviceB-10GE1/0/2] quit
[DeviceB] interface 10ge 1/0/3
[DeviceB-10GE1/0/3] traffic-policy p2 inbound
[DeviceB-10GE1/0/3] quit
[DeviceB] quit
```

# ----结束

# 检查配置结果

# 查看流分类的配置信息。

```
<DeviceB> display traffic classifier
Traffic Classifier Information:
  Classifier: c1
  Type: OR
  Rule(s):
    if-match vlan 10

Classifier: c2
  Type: OR
  Rule(s):
    if-match vlan 20
Total classifier number is 2
```

# # 查看流策略的配置信息。

```
<DeviceB> display traffic policy
Traffic Policy Information:
Policy: p1
Classifier: c1
   Type: OR
   Behavior: b1
   Remark:
    Remark 8021p 4

Policy: p2
Classifier: c2
   Type: OR
Behavior: b2
Remark:
   Remark 8021p 2
Total policy number is 2
```

# # 查看流策略的应用状态信息。

# 配置脚本

# DeviceB的配置脚本

```
sysname DeviceB
vlan batch 10 20 30
traffic classifier c1 type or
if-match vlan 10
traffic classifier c2 type or
if-match vlan 20
traffic behavior b1
remark 8021p 4
traffic behavior b2
remark 8021p 2
traffic policy p1
classifier c1 behavior b1 precedence 5
traffic policy p2
classifier c2 behavior b2 precedence 5
interface Vlanif10
ip address 192.168.10.1 255.255.255.0
interface Vlanif20
ip address 192.168.20.1 255.255.255.0
interface Vlanif30
ip address 192.168.100.1 255.255.255.0
interface 10GE1/0/1
```

```
port link-type trunk
port trunk allow-pass vlan 30

#
interface 10GE1/0/2
port default vlan 10
traffic-policy p1 inbound
#
interface 10GE1/0/3
port default vlan 20
traffic-policy p2 inbound
#
return
```

# **7** 报文重定向配置

7.1 报文重定向简介

7.2 报文重定向配置注意事项

7.3 配置基于MQC的报文重定向

7.4 举例:配置报文重定向到接口

7.5 举例: 配置报文重定向到下一跳

7.6 举例: 配置报文重定向到下一跳与NQA联动

7.7 举例:配置报文重定向实现路由选路

# 7.1 报文重定向简介

基于MQC实现的报文重定向,可以将符合流分类的报文流重新指定路径或方向,转发到指定的位置进行处理。

## 报文重定向包含以下动作:

- 重定向到接口:将需要由某个接口处理的报文,或者需要将通过某接口发送到指 定设备处理的报文,可以配置重定向到此接口。
- 重定向到下一跳:对于收到需要某台下游设备处理的报文时,可以通过配置重定向到该下游设备。重定向到下一跳的优先级高于直连路由、静态路由和通过动态路由协议生成的路由。若接收的报文匹配重定向到下一跳对应的流分类,则按照重定向到下一跳转发;若匹配失败,则根据目的地址按照正常转发流程转发。重定向到下一跳有时也被称为策略路由PBR(Policy-Based Routing)。

重定向到下一跳本身没有检测机制,如果对应的链路发生故障,重定向的下一跳地址不会自动改变,需要网络管理员介入或者等待重定向下一跳的ARP表项老化,这就无法保证链路及时切换,可能造成较长时间的业务中断。配置重定向到下一跳与NQA联动,可以检测重定向到下一跳的链路状态。当链路发生故障,重定向到下一跳会因为NQA检测失败而立即失效,从而缩短通信中断时间,提高服务质量。重定向到下一跳与NQA联动功能的实现机制如下:

- 若NQA测试例不存在或者类型不是ICMP类型,则检查失败,重定向到下一跳 配置失败。
- 若NQA测试例关联重定向到下一跳成功,链路检测正常,则重定向到下一跳 生效。

- 若NQA测试例关联重定向到下一跳成功,链路检测失败且探测次数超过设定值,则重定向到下一跳自动失效。
- 若NQA测试例关联重定向到下一跳成功,链路故障解除,链路恢复,则重定向到下一跳自动生效。

# 7.2 报文重定向配置注意事项

# License 依赖

报文重定向无需License许可即可使用。

# 硬件依赖

表 7-1 支持本特性的硬件

系列	支持产品
S5735-L-V2 series	S5735-L10T4X-A-V2/S5735-L14P2S-QA-V2/S5735-L16LP2UM2X-QA-V2/S5735-L16LP2X-QA-V2/S5735-L16P2UM2X-QA-V2/S5735-L16T4S-A-V2/S5735-L16T4X-QA-V2/S5735-L24P4S-A-V2/S5735-L24P4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L48LP4S-A-V2/S5735-L48LP4XE-A-V2/S5735-L48P4XE-A-V2/S5735-L48S4X-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L8P4X-A-V2/S5735-L8P4X-A-V2/S5735-L8P4X-A-V2/S5735-L8P4X-QA-V2/S5735-L8P4X-QA-V2/S5735-L8P4X-QA-V2/S5735-L8P4X-QA-V2/S5735-L8T4X-QA-V2
S5735-S-V2 series	S5735-S24HS4XE-V2/S5735-S24P4XE-V2/S5735- S24ST4XE-V2/S5735-S24T4XE-V2/S5735- S24U4XE-V2/S5735-S48HS4XE-V2/S5735- S48P4XE-V2/S5735-S48S4XE-V2/S5735-S48T4XE- V2/S5735-S48U4XE-V2
S5735I-L-V2 series	S5735I-L10T4X-A-V2/S5735I-L8P4X-A-V2
S5755-H series	S5755-H24N4Y-A/S5755-H24P4Y2CZ/S5755- H24T4Y2CZ/S5755-H24U4Y2CZ/S5755- H24UN4Y2CZ/S5755-H24UTM4X4Y2C/S5755- H48N4Y-A/S5755-H48P4Y2CZ/S5755-H48T4Y2CZ/ S5755-H48U4Y2CZ/S5755-H48UN4Y2CZ/S5755- H48UTM4X4Y2C
S6730-H-V2 series	S6730-H24X6C-V2/S6730-H28X6CZ-V2/S6730- H48X6C-V2/S6730-H48X6CZ-V2/S6730-H48Y6C- V2

系列	支持产品
S5732-H-V2 series	S5732-H24S4X6QZ-V2/S5732-H24UM4Y2CZ-KV2/ S5732-H24UM4Y2CZ-V2/S5732-H44S4X6QZ-V2/ S5732-H48UM4Y2CZ-KV2/S5732-H48UM4Y2CZ- V2
S5735I-H-V2 series	S5735I-H8T4S2XN-V2
S5735I-S-V2 series	S5735I-S24T4XE-V2/S5735I-S24U4XE-V2/S5735I- S8T4SN-V2/S5735I-S8T4XN-V2/S5735I-S8U4XN- V2

# 特性限制

表 7-2 本特性的使用限制

特性限制	系列	涉及产品
不支持通过流策略重定向BPDU报文。	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S5755-H series S6730-H-V2 series S5732-H-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735-S24HS4XE-V2/S5735-S24P4XE-V2/S5735-S24ST4XE-V2/S5735-S24T4XE-V2/S5735-S24U4XE-V2/S5735-S48HS4XE-V2/S5735-S48S4XE-V2/S5735-S48U4XE-S4-V2/S5735-S48U4XE-S4-V2/S5735-S48U4XE-S5735-S48U4XE-S5735-S48U4XE-S5735-S48U4XE-S5735-S48U4XE-S5735-S48U4XE-S5735-S5755-S57

特性限制	系列	涉及产品
		L48T4XE-A-V2/ S5735-L48T4XE- D-V2/S5735- L8P2T4X-A-V2/ S5735-L8P4S-A- V2/S5735-L8P4X- QA-V2/S5735- L8T4S-A-V2/ S5735-L8T4X-QA- V2
		S5735I-L10T4X-A- V2/S5735I-L8P4X- A-V2
		S5755-H24N4Y-A/ S5755- H24P4Y2CZ/ S5755- H24T4Y2CZ/ S5755- H24U4Y2CZ/ S5755- H24UN4Y2CZ/ S5755- H24UTM4X4Y2C/ S5755-H48N4Y-A/ S5755- H48T4Y2CZ/ S5755- H48UY2CZ/ S5755- H48UY2CZ/ S5755- H48UY2CZ/ S5755- H48UN4Y2CZ/
		S6730-H24X6C- V2/S6730- H28X6CZ-V2/ S6730-H48X6C- V2/S6730- H48X6CZ-V2/ S6730-H48Y6C-V2
		S5732- H24S4X6QZ-V2/ S5732- H24UM4Y2CZ- KV2/S5732- H24UM4Y2CZ-V2/ S5732-

特性限制	系列	涉及产品
		H44S4X6QZ-V2/ S5732- H48UM4Y2CZ- KV2/S5732- H48UM4Y2CZ-V2
		S5735I-S24T4XE- V2/S5735I- S24U4XE-V2/ S5735I-S8T4SN- V2/S5735I- S8T4XN-V2/ S5735I-S8U4XN- V2
		S5735I- H8T4S2XN-V2
对于S5735I-H-V2 Series: 重定向到接口的约束: - 重定向到接口仅支持入方向应用。 - 重定向到物理接口,出去的报文是转发编辑封装后的报文。 - 出接口需要在对应VLAN里面,流量才能出去。 - 重定向到接口不支持与deny配置在同一个流行为中。	S5735I-H- V2 series	S5735I- H8T4S2XN-V2

特性限制	系列	涉及产品
重定向动作和其他规则、动作叠加的约束: - 重定向后的报文无法通过URPF检查。 - 若流分类中配置if-match discard命令,则流行为中的重定向动作不生效。	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S5755-H series S6730-H-V2 series S5732-H-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735-S24HS4XE-V2/S5735-S24P4XE-V2/S5735-S24ST4XE-V2/S5735-S24T4XE-V2/S5735-S24U4XE-V2/S5735-S48HS4XE-V2/S5735-S48S4XE-V2/S5735-S48U4XE-V2/S5735-S48U4XE-V2/S5735-L10T4X-A-V2/S5735-L16LP2UM2X-QA-V2/S5735-L16LP2UM2X-QA-V2/S5735-L16P2UM2X-QA-V2/S5735-L16P2UM2X-QA-V2/S5735-L16P2UM2X-QA-V2/S5735-L24P4XE-A-V2/S5735-L24P4XE-A-V2/S5735-L24T4X

特性限制	系列	涉及产品
		S5735-L8P4S-A- V2/S5735-L8P4X- QA-V2/S5735- L8T4S-A-V2/ S5735-L8T4X-QA- V2
		S5735I-L10T4X-A- V2/S5735I-L8P4X- A-V2
		A-V2 S5755-H24N4Y-A/ S5755- H24P4Y2CZ/ S5755- H24U4Y2CZ/ S5755- H24UN4Y2CZ/ S5755- H24UTM4X4Y2C/ S5755- H24UTM4X4Y2C/ S5755- H48P4Y2CZ/ S5755- H48T4Y2CZ/ S5755- H48UN4Y2CZ/ S5755- H48UTM4X4Y2C
		V2/S6730- H28X6CZ-V2/ S6730-H48X6C- V2/S6730- H48X6CZ-V2/ S6730-H48Y6C-V2
		S5732- H24S4X6QZ-V2/ S5732- H24UM4Y2CZ- KV2/S5732- H24UM4Y2CZ-V2/ S5732- H44S4X6QZ-V2/ S5732-
		H48UM4Y2CZ-

特性限制	系列	涉及产品
		KV2/S5732- H48UM4Y2CZ-V2
		S5735I-S24T4XE- V2/S5735I- S24U4XE-V2/ S5735I-S8T4SN- V2/S5735I- S8T4XN-V2/ S5735I-S8U4XN- V2
		S5735I- H8T4S2XN-V2

特性限制	系列	涉及产品
对于S5735-S-V2 Series/S5735-L-V2 Series/S5735I-L-V2 Series/S5735I-L-V2 Series/S5735I-L-V2 Series/S5735I-L-V2 Series/S5735I-L-V2 Series:重定向下一跳的约束: - 重定向到下一跳不支持与deny配置在同一个流行为中。 - 不支持与匹配已知单播和未知单播的流分类叠加配置。 - 后策略路由(带low-precedence选项)不支持与匹配下一跳的流分类叠加配置。 - 仅支持入方向应用。对于S5735I-H-V2 Series:重定向下一跳的约束: - 重定向到下一跳不支持与deny配置在同一个流行为中。	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S5755-H series S6730-H-V2 series S5732-H-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735-S24HS4XE-V2/S5735-S24P4XE-V2/S5735-S24ST4XE-V2/S5735-S24T4XE-V2/S5735-S24U4XE-V2/S5735-S48HS4XE-V2/S5735-S48S4XE-V2/S5735-S48U4XE-SU2/S5735-S48U4XE-SU2/S5735-S48U4XE-SU2/S5735-S48U4XE-SU2/S5735-S48U4XE-SU2/S5735-S48U4XE-SU2/S5735-S48U4XE-SU2/S5735-S48U4XE-SU2/S5735-S48U4XE-SU2/S5735-

特性限制	系列	涉及产品
		S5735-L8P4S-A- V2/S5735-L8P4X- QA-V2/S5735- L8T4S-A-V2/ S5735-L8T4X-QA- V2
		S5735I-L10T4X-A- V2/S5735I-L8P4X- A-V2
		A-V2 S5755-H24N4Y-A/ S5755- H24P4Y2CZ/ S5755- H24U4Y2CZ/ S5755- H24UN4Y2CZ/ S5755- H24UTM4X4Y2C/ S5755- H24UTM4X4Y2C/ S5755- H48P4Y2CZ/ S5755- H48T4Y2CZ/ S5755- H48UN4Y2CZ/ S5755- H48UTM4X4Y2C
		V2/S6730- H28X6CZ-V2/ S6730-H48X6C- V2/S6730- H48X6CZ-V2/ S6730-H48Y6C-V2
		S5732- H24S4X6QZ-V2/ S5732- H24UM4Y2CZ- KV2/S5732- H24UM4Y2CZ-V2/ S5732- H44S4X6QZ-V2/ S5732-
		H48UM4Y2CZ-

特性限制	系列	涉及产品
		KV2/S5732- H48UM4Y2CZ-V2
		S5735I-S24T4XE- V2/S5735I- S24U4XE-V2/ S5735I-S8T4SN- V2/S5735I- S8T4XN-V2/ S5735I-S8U4XN- V2
		S5735I- H8T4S2XN-V2

# 7.3 配置基于 MQC 的报文重定向

# 背景信息

通过配置重定向,设备将符合流分类规则的报文重定向到指定接口和指定的下一跳地 址。

# □ 说明

- 对于二层数据流量,建议配置报文重定向到接口;对于三层数据流量,建议配置报文重定向 到下一跳。
- MQC相关的配置注意事项,请参考MQC章节的配置注意事项页面。

# 操作步骤

步骤1 配置流分类。

流分类的配置方式,请参考MQC配置中的3.4 配置流分类。

# 步骤2 配置流行为。

1. 进入系统视图。

system-view

2. 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。

traffic behavior behavior-name

- 3. 定义流行为中的重定向动作。
  - 重定向到指定接口

redirect interface interface-type interface-number [ fail-action forward ]

#### □ 说明

通常情况下,重定向报文到出接口时,出接口需要加入该报文所对应的VLAN。

- 重定向到单个下一跳IP地址

redirect [ vpn-instance vpn-instance-name ] nexthop { ip-address [ track nqa admin-name test-name [ reaction probe-failtimes fail-times ] ] } &<1-16> [ fail-action discard ] [ low-precedence ]

redirect ipv6 [ vpn-instance vpn-instance-name ] nexthop { ipv6-address [ track nqa adminname test-name [ reaction probe-failtimes fail-times ] ] } &<1-16> [ fail-action discard ]

- 重定向到多个下一跳IP地址

redirect load-balance [ vpn-instance vpn-instance-name ] nexthop { ip-address [ track nqa
admin-name test-name [ reaction probe-failtimes fail-times ] ] } &<1-16> [ fail-action
discard ] [ low-precedence ]

redirect ipv6 load-balance [vpn-instance vpn-instance-name] nexthop { ipv6-address [ track nqa admin-name test-name [ reaction probe-failtimes fail-times ] ] } &<1-16> [ fail-action discard ]

仅S5732-H-V2、S6730-H-V2、S5755-H、S5735-S-V2、S5735I-S-V2,、S5735I-H-V2支持重定向到多个下一跳IP地址。

- 重定向到远程下一跳

redirect remote [ vpn-instance vpn-instance-name ] { ip-address [ track nqa admin-name test-name [ reaction probe-failtimes fail-times ] ] } &<1-16> [ exact ] [ low-precedence ] redirect remote ipv6 [ vpn-instance vpn-instance-name ] ipv6-address &<1-16> [ exact ]

#### □ 说明

当指定参数**low-precedence**以配置下一跳为低优先级的下一跳(也称为后策略路由)时,设备不支持重定向IPv6报文和隧道封装格式的IP报文。

4. 退出流行为视图。

quit

#### 步骤3 配置流策略。

1. 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。

traffic policy policy-name

3. 退出流策略视图。

quit

#### 步骤4 应用流策略。

- 在全局上应用流策略。
  - a. 在全局上应用流策略。 traffic-policy *policy-name* global [ slot *slot-id* ] inbound
- 在接口上应用流策略。
  - a. 进入接口视图。

interface interface-type interface-number

b. 在接口上应用流策略。 traffic-policy policy-name inbound

c. 退出接口视图。 quit

在VLAN上应用流策略。

a. 创建VLAN,并进入VLAN视图。 vlan vlan-id

o. 在VLAN上应用流策略。

traffic-policy policy-name inbound

应用后,系统对属于该VLAN并匹配流分类中规则的入方向或出方向报文实施 策略控制。

c. 退出VLAN视图。 guit

#### ----结束

# 检查配置结果

操作	命令
查看已配置的流分类信息	display traffic classifier [ classifier- name ]
查看已配置的流行为信息	display traffic behavior [ behavior- name ]
查看已配置的流策略信息	display traffic policy [ policy-name [ classifier classifier-name ] ]
查看流策略的应用记录	display traffic-policy applied-record [ policy-name ]
查看TCAM下发失败的信息	display system tcam fail-record [ slot slot-id ]
查看不同的业务占用的组索引和规则计数	display system tcam service brief [ slot slot-id ]
	display system tcam service { cpcar slot slot-id   service-name slot slot-id [ chip chip-id ] }
查看流策略的应用数据	display system tcam service traffic- policy
查看规则命中的信息	display system tcam match-rules slot slot-id
查看应用流策略后的报文统计信息	display traffic-policy statistics
查看各视图下应用流策略时支持的匹配字 段和动作	display system tcam acl group- information
查看待应用的流策略所占用的资源信息, 以确认配置提交后对应的流策略是否能应 用成功	display traffic-policy pre-state

# 7.4 举例: 配置报文重定向到接口

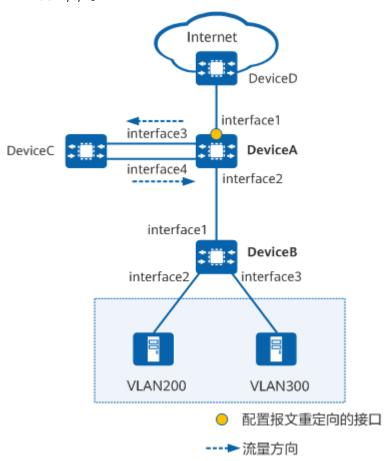
# 组网需求

如<mark>图7-1</mark>所示,服务器通过设备DeviceA、DeviceB和DeviceD与Internet进行通信。用户希望将来自Internet的所有流量重定向到DeviceC进行安全过滤,从而保证Internet 到服务器全部流量的安全性。

#### 图 7-1 配置报文重定向到接口组网图

# 山 说明

本例中interface1,interface2,interface3和interface4分别代表10GE1/0/1,10GE1/0/2,10GE1/0/3和10GE1/0/4。



# 操作步骤

步骤1 创建VLAN并配置各接口,保证二层网络互通

# 在DeviceB上创建VLAN200和VLAN300。

<HUAWEI> system-view [HUAWEI] sysname DeviceB [DeviceB] vlan batch 200 300 # 配置DeviceB的接口10GE1/0/1的接口类型为Trunk,并将10GE1/0/1加入VLAN200和VLAN300;配置DeviceB的接口10GE1/0/2和10GE1/0/3的接口类型为Access,并将10GE1/0/2加入VLAN200,10GE1/0/3加入VLAN300。

```
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] portswitch
[DeviceB-10GE1/0/1] port link-type trunk
[DeviceB-10GE1/0/1] port trunk allow-pass vlan 200 300
[DeviceB-10GE1/0/1] quit
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] portswitch
[DeviceB-10GE1/0/2] port link-type access
[DeviceB-10GE1/0/2] port default vlan 200
[DeviceB-10GE1/0/2] quit
[DeviceB] interface 10ge 1/0/3
[DeviceB-10GE1/0/3] portswitch
[DeviceB-10GE1/0/3] port link-type access
[DeviceB-10GE1/0/3] port default vlan 300
[DeviceB-10GE1/0/3] quit
```

# 在DeviceA上创建VLAN200和VLAN300。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 200 300
```

# 配置DeviceA的接口10GE1/0/1、10GE1/0/2、10GE1/0/3和10GE1/0/4的接口类型为Trunk,并将它们都加入VLAN200和VLAN300。为防止出现环路,将接口10GE1/0/3和10GE1/0/4加入同一个端口隔离组,并配置接口10GE1/0/4禁止MAC地址学习以防止MAC地址漂移。

```
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type trunk
[DeviceA-10GE1/0/1] port trunk allow-pass vlan 200 300
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port link-type trunk
[DeviceA-10GE1/0/2] port trunk allow-pass vlan 200 300
[DeviceA-10GE1/0/2] quit
[DeviceA] interface 10ge 1/0/3
[DeviceA-10GE1/0/3] portswitch
[DeviceA-10GE1/0/3] port link-type trunk
[DeviceA-10GE1/0/3] port trunk allow-pass vlan 200 300
[DeviceA-10GE1/0/3] port-isolate enable group 1
DeviceA-10GE1/0/3] quit
[DeviceA] interface 10ge 1/0/4
[DeviceA-10GE1/0/4] portswitch
[DeviceA-10GE1/0/4] port link-type trunk
[DeviceA-10GE1/0/4] port trunk allow-pass vlan 200 300
[DeviceA-10GE1/0/4] port-isolate enable group 1
[DeviceA-10GE1/0/4] mac-address learning disable
[DeviceA-10GE1/0/4] quit
```

#### 步骤2 在DeviceA上配置报文重定向到接口

# 配置流分类。流分类c1中的匹配规则为匹配所有报文。

```
[DeviceA] traffic classifier c1
[DeviceA-classifier-c1] if-match any
[DeviceA-classifier-c1] quit
```

# 配置流行为。流行为b1中的动作为重定向报文到指定接口。

```
[DeviceA] traffic behavior b1
[DeviceA-behavior-b1] redirect interface 10ge 1/0/3
[DeviceA-behavior-b1] quit
```

# # 创建流策略p1,将流分类c1和对应的流行为b1进行绑定。

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

# 在接口10GE1/0/1的入方向应用流策略。

```
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] traffic-policy p1 inbound
[DeviceA-10GE1/0/1] quit
```

## ----结束

# 检查配置结果

# # 查看流分类的配置信息。

```
<DeviceA> display traffic classifier
Traffic Classifier Information:
Classifier: c1
Type: OR
Rule(s):
if-match any
Trick by 15 (2)
```

Total classifier number is 1

## # 查看流行为的配置信息。

```
<DeviceA> display traffic behavior
Traffic Behavior Information:
Behavior: b1
Redirect:
Redirect interface 10GE1/0/3
```

Total behavior number is 1

# # 查看流策略的配置信息。

```
<DeviceA> display traffic policy
Traffic Policy Information:
Policy: p1
Classifier: c1
Type: OR
Behavior: b1
Redirect:
Redirect interface 10GE1/0/3
```

Total policy number is 1

#### # 查看流策略的应用状态信息。

```
<DeviceA> display traffic-policy applied-record

Total records : 1

Policy Type/Name Apply Parameter Slot State

p1 10GE1/0/1(IN) 1 success
```

# 配置脚本

## ● DeviceA的配置脚本

```
#
sysname DeviceA
#
vlan batch 200 300
```

```
traffic classifier c1 type or
if-match any
traffic behavior b1
redirect interface 10GE 1/0/3
traffic policy p1
classifier c1 behavior b1 precedence 5
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 200 300
traffic-policy p1 inbound
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 200 300
interface 10GE1/0/3
port link-type trunk
port trunk allow-pass vlan 200 300
port-isolate enable group 1
interface 10GE1/0/4
port link-type trunk
port trunk allow-pass vlan 200 300
port-isolate enable group 1
mac-address learning disable
return
```

#### DeviceB的配置脚本

```
#
sysname DeviceB
#
vlan batch 200 300
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 200 300
#
interface 10GE1/0/2
port default vlan 200
#
interface 10GE1/0/3
port default vlan 300
#
return
```

# 7.5 举例: 配置报文重定向到下一跳

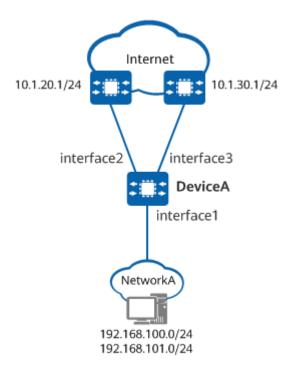
# 组网需求

如<mark>图7-2</mark>所示,DeviceA作为三层转发设备,与网络NetworkA之间路由可达,并且可以通过两条链路连接到Internet。两条链路中,一条是高速链路,网关为10.1.20.1/24;另外一条是低速链路,网关为10.1.30.1/24。用户希望通过DeviceA上送到Internet的报文中,源IP地址为192.168.100.0/24的报文通过高速链路传输,而源IP地址为192.168.101.0/24的报文则通过低速链路传输。

# 图 7-2 配置报文重定向到下一跳组网图

# □ 说明

本例中interface1,interface2,interface3分别代表10GE1/0/1,10GE1/0/2和10GE1/0/3。



# 操作步骤

## 步骤1 创建VLAN并配置各接口

# 在DeviceA上创建VLAN10、VLAN20和VLAN30。

<HUAWEI> system-view [HUAWEI] sysname DeviceA [DeviceA] vlan batch 10 20 30

# 配置DeviceA上接口10GE1/0/1、10GE1/0/2和10GE1/0/3的接口类型为Trunk,并加入VLAN。

```
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type trunk
[DeviceA-10GE1/0/1] port trunk allow-pass vlan 10
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port link-type trunk
[DeviceA-10GE1/0/2] port trunk allow-pass vlan 20
[DeviceA-10GE1/0/2] quit
[DeviceA] interface 10ge 1/0/3
[DeviceA-10GE1/0/3] portswitch
[DeviceA-10GE1/0/3] port link-type trunk
[DeviceA-10GE1/0/3] port link-type trunk
[DeviceA-10GE1/0/3] port trunk allow-pass vlan 30
[DeviceA-10GE1/0/3] quit
```

# 创建VLANIF10、VLANIF20、VLANIF30,并配置各虚拟接口IP地址。

```
[DeviceA] interface vlanif 10
[DeviceA-Vlanif10] ip address 10.1.10.2 24
[DeviceA-Vlanif10] quit
[DeviceA] interface vlanif 20
[DeviceA-Vlanif20] ip address 10.1.20.2 24
[DeviceA-Vlanif20] quit
[DeviceA] interface vlanif 30
[DeviceA-Vlanif30] ip address 10.1.30.2 24
[DeviceA-Vlanif30] quit
```

# 步骤2 配置ACL规则

# 在DeviceA上创建编码为3001、3002的高级ACL,规则分别为允许源IP地址为192.168.100.0/24和192.168.101.0/24的报文通过。

```
[DeviceA] acl 3001
[DeviceA-acl4-advance-3001] rule permit ip source 192.168.100.0 0.0.0.255
[DeviceA-acl4-advance-3001] quit
[DeviceA] acl 3002
[DeviceA-acl4-advance-3002] rule permit ip source 192.168.101.0 0.0.0.255
[DeviceA-acl4-advance-3002] quit
```

#### 步骤3 配置流分类

#在DeviceA上创建流分类c1和c2, 匹配规则分别为ACL 3001和ACL 3002。

```
[DeviceA] traffic classifier c1
[DeviceA-classifier-c1] if-match acl 3001
[DeviceA-classifier-c1] quit
[DeviceA] traffic classifier c2
[DeviceA-classifier-c2] if-match acl 3002
[DeviceA-classifier-c2] quit
```

## 步骤4 配置流行为

# 在DeviceA上创建流行为b1和b2,并分别指定重定向到10.1.20.1和10.1.30.1的动作。

```
[DeviceA] traffic behavior b1
[DeviceA-behavior-b1] redirect nexthop 10.1.20.1
[DeviceA-behavior-b1] quit
[DeviceA] traffic behavior b2
[DeviceA-behavior-b2] redirect nexthop 10.1.30.1
[DeviceA-behavior-b2] quit
```

# 步骤5 配置流策略并应用到接口上

# 在DeviceA上创建流策略p1,将流分类c1和流行为b1进行绑定,将流分类c2和流行为b2进行绑定。

```
[DeviceA] traffic policy p1
[DeviceA-trafficpolicy-p1] classifier c1 behavior b1
[DeviceA-trafficpolicy-p1] classifier c2 behavior b2
[DeviceA-trafficpolicy-p1] quit
```

# 将流策略p1应用到接口10GE1/0/1的入方向上。

```
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] traffic-policy p1 inbound
[DeviceA-10GE1/0/1] quit
```

## ----结束

# 检查配置结果

# 查看流分类的配置信息。

```
<DeviceA> display traffic classifier

Traffic Classifier Information:
Classifier: c1
Type: OR
Rule(s):
if-match acl 3001

Classifier: c2
Type: OR
Rule(s):
```

```
if-match acl 3002
```

Total classifier number is 2

# # 查看流策略的配置信息。

```
<DeviceA> display traffic policy
Traffic Policy Information:
Policy: p1
Classifier: c1
   Type: OR
   Behavior: b1
   Redirect:
    Redirect nexthop
   10.1.20.1

Classifier: c2
   Type: OR
   Behavior: b2
   Redirect:
   Redirect nexthop
   10.1.30.1
Total policy number is 2
```

# # 查看流策略的应用状态信息。

# 配置脚本

#### DeviceA的配置脚本

```
sysname DeviceA
vlan batch 10 20 30
acl number 3001
rule 5 permit ip source 192.168.100.0 0.0.0.255
acl number 3002
rule 5 permit ip source 192.168.101.0 0.0.0.255
traffic classifier c1 type or
if-match acl 3001
traffic classifier c2 type or
if-match acl 3002
traffic behavior b1
redirect nexthop 10.1.20.1
traffic behavior b2
redirect nexthop 10.1.30.1
traffic policy p1
classifier c1 behavior b1 precedence 5
classifier c2 behavior b2 precedence 10
interface Vlanif10
ip address 10.1.10.2 255.255.255.0
```

```
interface Vlanif20
ip address 10.1.20.2 255.255.255.0

#
interface Vlanif30
ip address 10.1.30.2 255.255.255.0

#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 10
traffic-policy p1 inbound

#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 20

#
interface 10GE1/0/3
port link-type trunk
port trunk allow-pass vlan 30

#
return
```

# 7.6 举例: 配置报文重定向到下一跳与 NQA 联动

# 组网需求

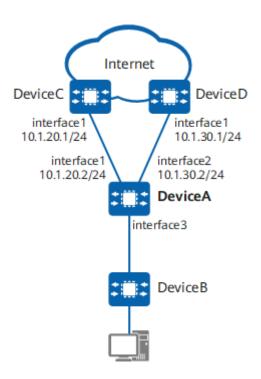
如<mark>图7-3</mark>所示,DeviceA是DeviceB的上层设备,DeviceB是用户网关,DeviceA与DeviceB之间路由可达。DeviceA通过两条链路连接到Internet,一条是高速链路,网关为10.1.20.1/24;另外一条是低速链路,网关为10.1.30.1/24。当前DeviceA已配置默认路由保证流量默认通过高速链路传输。用户希望实现如下需求:

- 通过报文重定向到下一跳将源IP地址为192.168.101.0/24的报文分流至低速链路传输,从而减少高速链路的带宽压力。
- 当低速链路出现故障的时候,希望源IP地址为192.168.101.0/24的报文能尽快切换回高速链路传输,尽量缩短由于链路故障导致的通信中断时间。

#### 图 7-3 配置报文重定向与 NQA 联动组网图

# 山 说明

本例中interface1, interface2, interface3分别代表10GE1/0/1, 10GE1/0/2和10GE1/0/3。



# 操作步骤

# 步骤1 创建VLAN并配置各接口

# #配置DeviceA。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 10 20 30
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type trunk
[DeviceA-10GE1/0/1] port trunk allow-pass vlan 10
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] port link-type trunk
[DeviceA-10GE1/0/2] port trunk allow-pass vlan 20
[DeviceA-10GE1/0/2] quit
[DeviceA] interface 10ge1/0/3
[DeviceA-10GE1/0/3] portswitch
[DeviceA-10GE1/0/3] port link-type trunk
[DeviceA-10GE1/0/3] port trunk allow-pass vlan 30
[DeviceA-10GE1/0/3] quit
[DeviceA] interface vlanif 10
[DeviceA-Vlanif10] ip address 10.1.20.2 24
[DeviceA-Vlanif10] quit
[DeviceA] interface vlanif 20
[DeviceA-Vlanif20] ip address 10.1.30.2 24
[DeviceA-Vlanif20] quit
[DeviceA] interface vlanif 30
[DeviceA-Vlanif30] ip address 10.1.10.2 24
[DeviceA-Vlanif30] quit
```

## #配置DeviceC。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceC
[DeviceC] vlan batch 10
[DeviceC] interface 10ge 1/0/1
[DeviceC-10GE1/0/1] portswitch
[DeviceC-10GE1/0/1] port link-type trunk
```

[DeviceC-10GE1/0/1] port trunk allow-pass vlan 10 [DeviceC-10GE1/0/1] quit [DeviceC] interface vlanif 10 [DeviceC-Vlanif10] ip address 10.1.20.1 24 [DeviceC-Vlanif10] quit

#### #配置DeviceD。

<HUAWEI> system-view
[HUAWEI] sysname DeviceD
[DeviceD] vlan batch 20
[DeviceD] interface 10ge 1/0/1
[DeviceD-10GE1/0/1] portswitch
[DeviceD-10GE1/0/1] port link-type trunk
[DeviceD-10GE1/0/1] port trunk allow-pass vlan 20
[DeviceD-10GE1/0/1] quit
[DeviceD] interface vlanif 20
[DeviceD-Vlanif20] ip address 10.1.30.1 24
[DeviceD-Vlanif20] quit

# 步骤2 在DeviceA上配置NQA测试例

[DeviceA] nqa test-instance user test
[DeviceA-nqa-user-test] test-type icmp
[DeviceA-nqa-user-test] destination-address ipv4 10.1.30.1
[DeviceA-nqa-user-test] frequency 11
[DeviceA-nqa-user-test] probe-count 2
[DeviceA-nqa-user-test] interval seconds 5
[DeviceA-nqa-user-test] timeout 4
[DeviceA-nqa-user-test] start now
[DeviceA-nqa-user-test] quit

#### 步骤3 配置ACL规则

# 在DeviceA上创建ACL 3001, 规则为允许源IP地址为192.168.101.0/24的报文通过。

[DeviceA] acl 3001 [DeviceA-acl4-advance-3001] rule permit ip source 192.168.101.0 0.0.0.255 [DeviceA-acl4-advance-3001] quit

#### 步骤4 配置流分类

#在DeviceA上创建流分类c1,匹配规则为ACL 3001。

[DeviceA] traffic classifier c1 [DeviceA-classifier-c1] if-match acl 3001 [DeviceA-classifier-c1] quit

#### 步骤5 配置流行为

#在DeviceA上创建流行为b1,指定重定向到10.1.30.1的动作,并联动NQA测试例。

[DeviceA] **traffic behavior b1**[DeviceA-behavior-b1] **redirect nexthop 10.1.30.1 track nqa user test**[DeviceA-behavior-b1] **quit** 

# 步骤6 配置流策略并将流策略应用到接口上

# 在DeviceA上创建流策略p1,将流分类c1和流行为b1进行绑定。

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

#将流策略p1应用到接口10GE1/0/3的入方向上。

[DeviceA] interface 10ge 1/0/3 [DeviceA-10GE1/0/3] traffic-policy p1 inbound [DeviceA-10GE1/0/3] quit [DeviceA] quit

#### ----结束

# 检查配置结果

# 查看ACL规则的配置信息。

```
<DeviceA> display acl 3001
Advanced ACL 3001, 1 rule
ACL's step is 5
rule 5 permit ip source 192.168.101.0 0.0.0.255 (0 times matched)
```

## # 查看流分类的配置信息。

```
<DeviceA> display traffic classifier
Traffic Classifier Information:
Classifier: c1
Type: OR
Rule(s):
if-match acl 3001

Total classifier number is 1
```

# # 查看流策略的配置信息。

# <DeviceA> display traffic policy Traffic Policy Information: Policy: p1 Classifier: c1 Type: OR Behavior: b1 Redirect:

Redirect nexthop 10.1.30.1 track nga user test

Total policy number is 1

# # 查看流策略的应用状态信息。

# 查看NQA测试结果。可以看到"Completion:success"、"Lost packet ratio: 0%",这说明NQA测试结果成功,链路没有发生故障。

## <DeviceA> display nqa results test-instance user test

```
NQA entry(user, test) :test flag is active ,test type is ICMP
1 . Test 1 result The test is finished
 Send operation times: 2
                                Receive response times: 2
 Completion:success
                                RTD over thresholds number: 0
                                Drop operation number:0
 Attempts number:1
 Disconnect operation number:0
                                    Operation timeout number:0
                                    Connection fail number:0
 System busy operation number:0
 Operation sequence errors number:0 RTT Status errors number:0
 Destination IP address:10.1.30.1
 Min/Max/Average completion time: 3/4/3
 Sum/Square-Sum completion time: 7/25
 Last response packet receiving tim: 2020-04-09 09:55:38.2
 Lost packet ratio: 0 %
```

# 配置脚本

#### ● DeviceA的配置脚本

```
sysname DeviceA
vlan batch 10 20 30
acl number 3001
rule 5 permit ip source 192.168.101.0 0.0.0.255
traffic classifier c1 type or
if-match acl 3001
traffic behavior b1
redirect nexthop 10.1.30.1 track nga user test
traffic policy p1
classifier c1 behavior b1 precedence 5
interface Vlanif10
ip address 10.1.20.2 255.255.255.0
interface Vlanif20
ip address 10.1.30.2 255.255.255.0
interface Vlanif30
ip address 10.1.10.2 255.255.255.0
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 10
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 20
interface 10GE1/0/3
port link-type trunk
port trunk allow-pass vlan 30
traffic-policy p1 inbound
nqa test-instance user test
test-type icmp
destination-address ipv4 10.1.30.1
interval seconds 5
timeout 4
probe-count 2
frequency 11
start now
return
```

# ● DeviceC的配置脚本

```
#
sysname DeviceC
#
vlan batch 10
#
interface Vlanif10
ip address 10.1.20.1 255.255.255.0
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 10
#
return
```

#### ● DeviceD的配置脚本

```
#
sysname DeviceD
#
vlan batch 20
#
interface Vlanif20
ip address 10.1.30.1 255.255.255.0
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 20
#
return
```

# 7.7 举例: 配置报文重定向实现路由选路

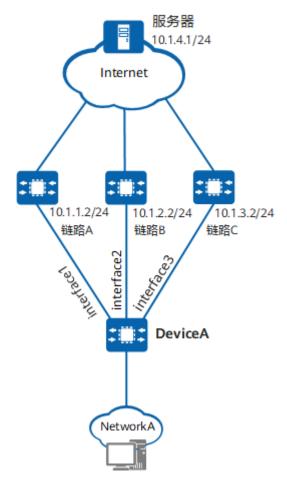
# 组网需求

如<mark>图7-4</mark>所示,由于不同的链路质量等因素,用户要求如果PC需要访问服务器,优先选择链路A,其次选择链路B,最后选择缺省的链路C。

# 图 7-4 配置报文重定向实现路由选路组网图

# □ 说明

本例中interface1, interface2, interface3分别代表10GE1/0/1, 10GE1/0/2和10GE1/0/3。



# 配置思路

采用如下思路在DeviceA上配置报文重定向到下一跳,实现路由选路:

- 1. 通过路由协议生成或者静态配置到达服务器的路由,指定下一跳为10.1.1.2/24, 从链路A通过。
- 2. 配置匹配服务器所在网段的报文重定向到下一跳,下一跳为10.1.2.2/24,从链路B通过;指定该下一跳为低优先级的下一跳,并在绑定流分类和流行为时指定流分类的优先级为高优先级,以实现优选通过链路A的路由。
- 3. 配置匹配全网段的报文重定向到下一跳代替缺省路由,下一跳为10.1.3.2/24,从 链路C通过;指定该下一跳为低优先级的下一跳,并在绑定流分类和流行为时指定 流分类的优先级为低优先级,以实现优选通过链路A和链路B的路由。

配置完成后,DeviceA的路由转发将按"路由协议生成或者静态配置的路由">"匹配服务器所在网段的报文重定向到下一跳">"匹配全网段的报文重定向到下一跳"的先后顺序进行选路。

# 操作步骤

# 步骤1 创建VLAN并配置各接口

# 在DeviceA上创建VLAN10、VLAN20、VLAN30。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 10 20 30
```

# 配置DeviceA上接口10GE1/0/1、10GE1/0/2和10GE1/0/3的接口类型为Trunk,并分别加入VLAN10、VLAN20和VLAN30。

```
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type trunk
[DeviceA-10GE1/0/1] port trunk allow-pass vlan 10
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port link-type trunk
[DeviceA-10GE1/0/2] port link-type trunk
[DeviceA-10GE1/0/2] quit
[DeviceA-10GE1/0/3] quit
[DeviceA-10GE1/0/3] portswitch
[DeviceA-10GE1/0/3] port link-type trunk
[DeviceA-10GE1/0/3] port link-type trunk
[DeviceA-10GE1/0/3] port trunk allow-pass vlan 30
[DeviceA-10GE1/0/3] quit
```

# 创建接口VLANIF10、VLANIF20和VLANIF30,并配置IP地址。

```
[DeviceA] interface vlanif 10
[DeviceA-Vlanif10] ip address 10.1.1.1 24
[DeviceA-Vlanif10] quit
[DeviceA] interface vlanif 20
[DeviceA-Vlanif20] ip address 10.1.2.1 24
[DeviceA-Vlanif20] quit
[DeviceA] interface vlanif 30
[DeviceA-Vlanif30] ip address 10.1.3.1 24
[DeviceA-Vlanif30] quit
```

#### 步骤2 配置到达服务器的静态路由

# 配置到达服务器的静态路由,下一跳为10.1.1.2。

[DeviceA] ip route-static 10.1.4.0 24 10.1.1.2

# 步骤3 配置流分类

# 在DeviceA上创建ACL 3001和ACL 3002,规则分别为允许目的地址为10.1.4.0/24、0.0.0.0/0网段的报文通过。

[DeviceA] acl 3001

[DeviceA-acl4-advance-3001] rule permit ip destination 10.1.4.0 0.0.0.255

[DeviceA-acl4-advance-3001] quit

[DeviceA] acl 3002

[DeviceA-acl4-advance-3002] rule permit ip destination 0.0.0.0 255.255.255.255

[DeviceA-acl4-advance-3002] quit

# 在DeviceA上创建流分类c1、c2,分别匹配规则为ACL 3001、ACL 3002,并且指定流分类c1的优先级高于流分类c2的优先级。

[DeviceA] traffic classifier c1

[DeviceA-classifier-c1] if-match acl 3001

[DeviceA-classifier-c1] quit

[DeviceA] traffic classifier c2

[DeviceA-classifier-c2] if-match acl 3002

[DeviceA-classifier-c2] quit

#### 步骤4 配置流行为

# 在DeviceA上创建流行为b1和b2,指定报文重定向的下一跳分别为10.1.2.2和 10.1.3.2,并且指定优先级均为**low-preference**,使报文重定向到下一跳的优先级比动态路由协议生成或者静态手工配置的路由优先级低。

[DeviceA] traffic behavior b1

[DeviceA-behavior-b1] redirect nexthop 10.1.2.2 low-precedence

[DeviceA-behavior-b1] quit

[DeviceA] traffic behavior b2

[DeviceA-behavior-b2] redirect nexthop 10.1.3.2 low-precedence

[DeviceA-behavior-b2] quit

# 步骤5 配置流策略

# 在DeviceA上创建流策略p1,将流分类和对应的流行为进行绑定。

[DeviceA] traffic policy p1

[DeviceA-trafficpolicy-p1] classifier c1 behavior b1 precedence 5

[DeviceA-trafficpolicy-p1] classifier c2 behavior b2 precedence 10

[DeviceA-trafficpolicy-p1] quit

#将流策略p1应用到全局。配置完成后,DeviceA所接收的报文都会匹配流策略p1。

[DeviceA] traffic-policy p1 global inbound

[DeviceA] quit

#### ----结束

# 检查配置结果

# 查看ACL规则的配置信息。

<DeviceA> display acl 3001

Advanced ACL 3001, 1 rule

ACL's step is 5

rule 5 permit ip destination 10.1.4.0 0.0.0.255 (0 times matched)

<DeviceA> display acl 3002

Advanced ACL 3002, 1 rule

ACL's step is 5

rule 5 permit ip (0 times matched)

# 查看流分类的配置信息。

#### <DeviceA> display traffic classifier

Traffic Classifier Information:

```
Classifier: c1
    Type: OR
    Rule(s):
     if-match acl 3001
  Classifier: c2
    Type: OR
    Rule(s):
     if-match acl 3002
Total classifier number is 2
```

#### # 查看流策略的配置信息。

```
<DeviceA> display traffic policy
 Traffic Policy Information:
  Policy: p1
    Classifier: c1
     Type: OR
    Behavior: b1
     Redirect:
      Redirect nexthop
      10.1.2.2
   Classifier: c2
     Type: OR
    Behavior: b2
     Redirect:
      Redirect nexthop
      10.1.3.2
Total policy number is 2
```

# # 查看流策略的应用状态信息。

```
<DeviceA> display traffic-policy applied-record
Total records: 1
                          Apply Parameter Slot State
Policy Type/Name
p1
                     Global(IN)
                                1 success
```

# 配置脚本

#### DeviceA的配置脚本

```
sysname DeviceA
vlan batch 10 20 30
traffic-policy p1 global inbound
acl number 3001
rule 5 permit ip destination 10.1.4.0 0.0.0.255
acl number 3002
rule 5 permit ip
traffic classifier c1 type or
if-match acl 3001
traffic classifier c2 type or
if-match acl 3002
traffic behavior b1
redirect nexthop 10.1.2.2 low-precedence
traffic behavior b2
```

```
redirect nexthop 10.1.3.2 low-precedence
traffic policy p1
classifier c1 behavior b1 precedence 5
classifier c2 behavior b2 precedence 10
interface Vlanif10
ip address 10.1.1.1 255.255.255.0
interface Vlanif20
ip address 10.1.2.1 255.255.255.0
interface Vlanif30
ip address 10.1.3.1 255.255.255.0
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 10
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 20
interface 10GE1/0/3
port link-type trunk
port trunk allow-pass vlan 30
ip route-static 10.1.4.0 255.255.255.0 10.1.1.2
return
```

# 8 优先级映射配置

- 8.1 优先级映射简介
- 8.2 优先级映射原理描述
- 8.3 优先级映射配置注意事项
- 8.4 优先级映射缺省配置
- 8.5 配置基于DiffServ域的优先级映射
- 8.6 配置端口优先级
- 8.7 配置本设备发送的协议报文的内部优先级
- 8.8 配置内部优先级与队列的映射关系
- 8.9 配置报文的优先级
- 8.10 优先级映射常见配置错误

# 8.1 优先级映射简介

# 定义

优先级映射用来实现报文携带的外部优先级与设备的内部优先级之间的转换,并利用 DiffServ域来管理和记录外部优先级和内部优先级之间的映射关系,从而设备可以根据 内部优先级提供有差别的QoS服务质量。

# 对于不同的优先级概念介绍如下:

• 外部优先级

又称为报文优先级、QoS优先级,即使用报文中某些特定字段比如VLAN报文的802.1p值、IP报文的DSCP值等记录QoS信息。需要注意的是,设备只可以根据设备内部优先级处理收到的报文,为不同的业务提供不同的QoS服务,所以上述外部优先级在进入设备后会映射为设备内部的优先级。

• 内部优先级

又称为服务等级(Class of Service)、PHB行为(Per-Hop Behavior)、本地优先级,支持8种取值,优先级从高到低依次为CS7、CS6、EF、AF4、AF3、AF2、AF1、BE,与出端口的8个队列从高到低依次对应。因此内部优先级决定了报文在

设备内部所属的队列。当针对某一个队列配置QoS业务时,即对所有通过该队列 转发的报文都设置了相同的QoS服务。

#### ● 丟弃优先级

又称为颜色(Color),是指报文在设备内部的丢弃优先级,用于决定当一个队列发生拥塞时报文的丢弃顺序,对内部优先级与队列的映射关系没有影响,丢弃优先级有3种取值,IEEE定义的优先级从低到高依次为Green、Yellow、Red。缺省情况下,丢弃优先级越高,则队列发生拥塞时,对应优先级的报文会被优先丢弃。

然而报文是否会被优先丢弃实际取决于参数的配置。例如,配置WRED丢弃模板中Green最大只能使用50%缓存,Red最大可以使用100%缓存,则队列发生拥塞时,标记为Green的报文将比标记为Red的报文优先丢弃。

# 目的

用户可以根据网络规划在不同网络中使用不同的外部优先级字段,例如在VLAN网络中使用802.1p,IP网络中使用DSCP。当报文在网络中传输时:

- 所有进入设备的报文,其外部优先级字段(包括802.1p、DSCP)都被映射为内部 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、拥塞管理等处理。
- 设备发出报文时,则将内部优先级映射为某种外部优先级字段,以便其他设备根据报文的外部优先级提供相应的QoS服务。

# 8.2 优先级映射原理描述

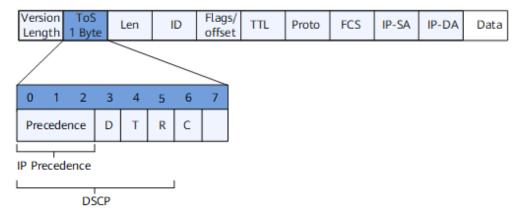
# 外部优先级字段

为了在Internet上针对不同的业务提供有差别的QoS服务质量,用户通过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8-1所示。

图 8-1 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Precedence字段外,ToS域中还包括D、T、R三个比特:

- D比特表示延迟要求(Delay, O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

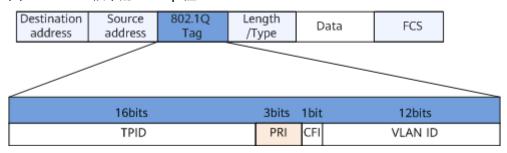
RFC1349重新定义了IP报文中的ToS域,增加了C比特,表示传输开销(Monetary Cost)。之后,IETF DiffServ工作组在RFC2474中将IPv4报文头ToS域中的比特0~5重新定义为DSCP,并将ToS域改名为DS(Differentiated Service)字节。DSCP在报文中的位置如图8-1所示。

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802.1p值位置如图8-2所示。

图 8-2 VLAN 帧中的 802.1p 值



在802.1Q头部中包含3比特长的PRI字段和1比特长的CFI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。CFI字段可以用来标识报文的丢弃优先级。

# 工作流程

如图8-3所示,用户从主机上获取语音、视频、数据三大类业务,主机上的流量通过 DeviceA和DeviceB传输到Network另一侧的用户。现在需要在整个网络中对三类业务 区分优先级,保证语音优先级一直最高、视频其次、数据优先级最低,这样设备可以 根据优先级的高低对三类业务提供不同的QoS服务。

不同网络中的报文使用不同的优先级字段,例如二层网络中的报文使用802.1p值,三层网络中的报文使用DSCP值。报文在进入设备时,设备将报文携带的外部优先级映射到内部优先级和丢弃优先级,再根据内部优先级和丢弃优先级对报文进行不同的QoS服务。报文在出设备时,设备可以根据内部优先级和丢弃优先级重标记报文外部优先级,以便后续网络根据报文外部优先级进行QoS服务。

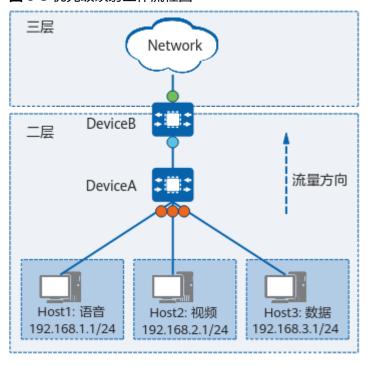


图 8-3 优先级映射工作流程图

- 入方向配置基于流的重标记优先级
- 入方向配置802.1p到内部优先级和丢弃优先级的映射
- 出方向根据内部优先级和丢弃优先级重标记DSCP

#### 优先级映射的工作流程说明如下:

- 1. DeviceA入方向配置流策略将语音、视频、数据三类业务重标记为不同的802.1p值,其中语音优先级最高、视频其次、数据最低。
- DeviceB入方向将802.1p值映射为内部优先级和丢弃优先级,DeviceB根据内部优 先级和丢弃优先级为报文提供不同的QoS服务。
- 3. DeviceB出方向根据内部优先级和丢弃优先级重标记DSCP值,以便后续三层网络根据DSCP值为三类业务提供不同的QoS服务。

# 8.3 优先级映射配置注意事项

# License 依赖

优先级映射无需License许可即可使用。

# 硬件依赖

表 8-1 支持本特性的硬件

系列	支持产品
S5735-L-V2 series	S5735-L10T4X-A-V2/S5735-L14P2S-QA-V2/S5735-L16LP2UM2X-QA-V2/S5735-L16LP2X-QA-V2/S5735-L16P2UM2X-QA-V2/S5735-L16T4S-A-V2/S5735-L16T4X-QA-V2/S5735-L24P4S-A-V2/S5735-L24P4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L48LP4S-A-V2/S5735-L48LP4XE-A-V2/S5735-L48P4XE-A-V2/S5735-L48S4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L8P2T4X-A-V2/S5735-L8P4S-A-V2/S5735-L8P4X-QA-V2/S
S5735-S-V2 series	S5735-S24HS4XE-V2/S5735-S24P4XE-V2/S5735- S24ST4XE-V2/S5735-S24T4XE-V2/S5735- S24U4XE-V2/S5735-S48HS4XE-V2/S5735- S48P4XE-V2/S5735-S48S4XE-V2/S5735-S48T4XE- V2/S5735-S48U4XE-V2
S5735I-L-V2 series	S5735I-L10T4X-A-V2/S5735I-L8P4X-A-V2
S5755-H series	S5755-H24N4Y-A/S5755-H24P4Y2CZ/S5755- H24T4Y2CZ/S5755-H24U4Y2CZ/S5755- H24UN4Y2CZ/S5755-H24UTM4X4Y2C/S5755- H48N4Y-A/S5755-H48P4Y2CZ/S5755-H48T4Y2CZ/ S5755-H48U4Y2CZ/S5755-H48UN4Y2CZ/S5755- H48UTM4X4Y2C
S6730-H-V2 series	S6730-H24X6C-V2/S6730-H28X6CZ-V2/S6730- H48X6C-V2/S6730-H48X6CZ-V2/S6730-H48Y6C- V2
S5732-H-V2 series	S5732-H24S4X6QZ-V2/S5732-H24UM4Y2CZ-KV2/ S5732-H24UM4Y2CZ-V2/S5732-H44S4X6QZ-V2/ S5732-H48UM4Y2CZ-KV2/S5732-H48UM4Y2CZ- V2
S5735I-H-V2 series	S5735I-H8T4S2XN-V2
S5735I-S-V2 series	S5735I-S24T4XE-V2/S5735I-S24U4XE-V2/S5735I- S8T4SN-V2/S5735I-S8T4XN-V2/S5735I-S8U4XN- V2

# 特性限制

表 8-2 本特性的使用限制

特性	特性限制	系列	涉及产品
端优级口先	对于S5735-S-V2 Series/S5735-L-V2 Series/S5735I-L-V2 Series/S5735I-S-V2 Series/S5735I-H-V2 Series: 切片使能的接口,不能配置出方向PHB映射使能,同时,出方向PHB使能的接口不能使能切片	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735- S24HS4XE -V2/ S5735- S24P4XE- V2/ S5735- S24ST4XE -V2/ S5735- S24T4XE- V2/ S5735- S24U4XE- V2/ S5735- S48HS4XE -V2/ S5735- S48P4XE- V2/ S5735- S48S4XE- V2/ S5735- S48S4XE- V2/ S5735- S48S4XE- V2/ S5735- S48T4XE- V2/ S5735- S48T4XE- V2/ S5735- S48U4XE- V2/ S5735- S48U4XE- V2/ S5735- S48U4XE- V2/ S5735- S48U4XE- V2/ S5735- S48U4XE- V2/ S5735- S48U4XE- V2/ S5735- L10T4X- A-V2/ S5735- L10T4X- A-V2/ S5735- L10T4X- A-V2/ S5735- L16LP2U M2X-QA- V2/ S5735- L16LP2U M2X-QA- V2/ S5735- L16LP2U M2X-QA- V2/ S5735- L16LP2U M2X-QA- V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/ S5735- L16LP2X- QA-V2/

V2/ S5735- L16T4S- A-V2/ S5735- L16T4X- QA-V2/ S5735- L24P4S- A-V2/ S5735- L24P4XE- A-V2/ S5735- L24T4XE- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4XE- A-V2/ S5735- S735- S735- S735- S735- S735- S735- S735- S735-

特性	特性限制	系列	涉及产品
			L48T4XE- D-V2/ S5735- L8P2T4X- A-V2/ S5735- L8P4S-A- V2/ S5735- L8P4X- QA-V2/ S5735- L8T4S-A- V2/ S5735- L8T4X- QA-V2/ S5735- L8T4X- QA-V2/
			A-V2/ S5735I- L8P4X-A- V2 S5735I- S24T4XE- V2/ S5735I- S24U4XE- V2/ S5735I- S8T4SN- V2/ S5735I- S8T4XN- V2/ S5735I- S8U4XN- V2/ S5735I- S8U4XN- V2 S5735I- S8U4XN- V2

特性	特性限制	系列	涉及产品
端优级	设备中缺省存在一个名为default的DiffServ域。除了这个域,设备其他DiffServ域可创建和删除。对于预先设定的default域,用户只能修改其映射关系,不能删除。	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S5755-H series S6730-H-V2 series S5732-H-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735- S24HS4XE-V2/ S5735- S24P4XE-V2/ S5735- S24ST4XE-V2/ S5735- S24U4XE-V2/ S5735- S24U4XE-V2/ S5735- S48HS4XE-V2/ S5735- S48P4XE-V2/ S5735- S48S4XE-V2/ S5735- S48U4XE-V2/ S5735- S48U4XE-V2/ S5735- L10T4X- A-V2/ S5735- L14P2S- QA-V2/ S5735- L16LP2U M2X-QA-V2/ S5735- L16LP2X- QA-V2/

特性	特性限制	系列	涉及产品
特性	特性限制	系列	S5735- L16T4X- QA-V2/ S5735- L24P4S- A-V2/ S5735- L24P4XE- A-V2/ S5735- L24T4S- A-V2/ S5735- L24T4X- QA-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- D-V2/ S5735- L24T4XE- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4XE- A-V2/ S5735- L48LP4XE- A-V2/ S5735- L48S4X- S5735- S
			S5735- L48T4XE- D-V2/ S5735- L8P2T4X-

特性	特性限制	系列	涉及产品
			S5755- H48UTM 4X4Y2C
			S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730- H48Y6C- V2
			S5732- H24S4X6 QZ-V2/ S5732- H24UM4 Y2CZ- KV2/ S5732- H24UM4 Y2CZ-V2/ S5732- H44S4X6 QZ-V2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/
			S5735I- S24T4XE- V2/ S5735I- S24U4XE- V2/ S5735I- S8T4SN- V2/ S5735I- S8T4XN- V2/

特性	特性限制	系列	涉及产品
			S5735I- S8U4XN- V2
			S5735I- H8T4S2X N-V2

特性	特性限制	系列	涉及产品
端优级	三层物理接口的端口优先级值为0,不能配置。	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S5755-H series S6730-H-V2 series S5732-H-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735- S24HS4XE -V2/ S5735- S24P4XE- V2/ S5735- S24ST4XE -V2/ S5735- S24T4XE- V2/ S5735- S24U4XE- V2/ S5735- S48HS4XE -V2/ S5735- S48S4XE- V2/ S5735- S48S4XE- V2/ S5735- S48U4XE- V2/ S5735- S48T4XE- V2/ S5735- S48T4XE- V2/ S5735- S48T4XE- V2/ S5735- S48U4XE- V2/ S5735- S48U4XE- V2/ S5735- L10T4X- A-V2/ S5735- L10T4X- A-V2/ S5735- L16LP2U M2X-QA- V2/ S5735- L16LP2X- QA-V2/

特性	特性限制	系列	涉及产品
特性	特性限制	系列	S5735- L16T4X- QA-V2/ S5735- L24P4S- A-V2/ S5735- L24P4XE- A-V2/ S5735- L24T4S- A-V2/ S5735- L24T4X- QA-V2/ S5735- L24T4XE- A-V2/ S5735- L24T4XE- D-V2/ S5735- L24T4XE- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4S- A-V2/ S5735- L48LP4XE- A-V2/ S5735- L48LP4XE- A-V2/ S5735- L48S4X- S5735- S
			S5735- L48T4XE- D-V2/ S5735- L8P2T4X-

特性	特性限制	系列	涉及产品
特性	特性限制	系列	S5755- H48UTM 4X4Y2C S6730- H24X6C- V2/ S6730- H28X6CZ- V2/ S6730- H48X6C- V2/ S6730- H48X6CZ- V2/ S6730- H48X6CZ- V2/ S6730- H48X6CZ- V2/ S6730- H48Y6C- V2/ S6730-
			H24S4X6 QZ-V2/ S5732- H24UM4 Y2CZ- KV2/ S5732- H24UM4 Y2CZ-V2/ S5732- H44S4X6 QZ-V2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ- KV2/ S5732- H48UM4 Y2CZ-
			S5735I- S24T4XE- V2/ S5735I- S24U4XE- V2/ S5735I- S8T4SN- V2/ S5735I- S8T4XN- V2/

特性	特性限制	系列	涉及产品
			S5735I- S8U4XN- V2
			S5735I- H8T4S2X N-V2

# 8.4 优先级映射缺省配置

优先级映射的主要缺省配置如表8-3所示。

表 8-3 优先级映射缺省配置

参数	缺省配置
优先级信任模式	报文数据流进入设备接口之后:     二层转发时     若报文携带VLAN Tag,缺省信任报文的外层802.1p值;若报文没有携带VLAN Tag,报文会根据缺省的端口优先级进行转发。     三层转发时 缺省信任DSCP值。
接口出方向报文的PHB到DSCP值的映射 功能	未使能
接口出方向报文的PHB到802.1p值的映 射功能	已使能
接口上应用的DiffServ域	default域
端口优先级	0

另外,从接收报文到转发报文的过程中,设备上定义了一系列缺省的报文优先级映射 关系,对报文进行优先级映射时,需要参考设备本身的缺省映射关系。

# 端口入方向报文优先级缺省映射关系

VLAN报文进入设备时,报文中802.1p值与设备内部优先级/丢弃优先级的缺省映射关系如表8-4所示。

#### □说明

端口优先级到服务等级(PHB行为)/颜色的映射关系与802.1p到服务等级(PHB行为)/颜色的映射关系一致。

表 8-4 入方向上 802.1p 值与设备内部优先级/丢弃优先级的映射关系

802.1p值	设备内部优先级(服务等 级)	设备内部丢弃优先级(颜 色)
0	BE	green
1	AF1	green
2	AF2	green
3	AF3	green
4	AF4	green
5	EF	green
6	CS6	green
7	CS7	green

IP报文进入设备时,报文中DSCP值与设备内部优先级/丢弃优先级的缺省映射关系如<mark>表8-5</mark>所示。

表 8-5 入方向上 DSCP 值与设备内部优先级/丢弃优先级的映射关系

DSCP值	设备内部优先级 (服务等级)	设备内 部丟弃 优先级 (颜 色)	DSCP	设备内部优先级 (服务等级)	设备内 部丟弃 优先级 (颜 色)
0	ВЕ	green	32	AF4	green
1	ВЕ	green	33	AF4	green
2	ВЕ	green	34	AF4	green
3	BE	green	35	AF4	green
4	BE	green	36	AF4	yellow
5	BE	green	37	AF4	green
6	BE	green	38	AF4	red
7	BE	green	39	AF4	green
8	AF1	green	40	EF	green
9	AF1	green	41	EF	green
10	AF1	green	42	EF	green
11	AF1	green	43	EF	green
12	AF1	yellow	44	EF	green

DSCP值	设备内部优先级 (服务等级)	设备内 部丟弃 优先级 (颜 色)	DSCP	设备内部优先级 (服务等级)	设备内 部丟弃 优先级 (颜 色)
13	AF1	green	45	EF	green
14	AF1	red	46	EF	green
15	AF1	green	47	EF	green
16	AF2	green	48	CS6	green
17	AF2	green	49	CS6	green
18	AF2	green	50	CS6	green
19	AF2	green	51	CS6	green
20	AF2	yellow	52	CS6	green
21	AF2	green	53	CS6	green
22	AF2	red	54	CS6	green
23	AF2	green	55	CS6	green
24	AF3	green	56	CS7	green
25	AF3	green	57	CS7	green
26	AF3	green	58	CS7	green
27	AF3	green	59	CS7	green
28	AF3	yellow	60	CS7	green
29	AF3	green	61	CS7	green
30	AF3	red	62	CS7	green
31	AF3	green	63	CS7	green

# 设备内部优先级与端口队列索引关系

设备内部优先级决定了设备将报文从端口下哪个队列转发出去,设备内部优先级与各队列之间的对应关系如**表8-6**所述。

表 8-6 设备内部优先级与各队列之间的对应关系表

设备内部优先级(服务等级)	队列索引
BE	0
AF1	1

设备内部优先级(服务等级)	队列索引
AF2	2
AF3	3
AF4	4
EF	5
CS6	6
CS7	7

# 端口出方向报文优先级缺省映射关系

VLAN报文从设备转发出去时,设备内部优先级/丢弃优先级与报文中802.1p值的缺省映射关系如表8-7所示。

表 8-7 出方向上设备内部优先级/丢弃优先级与 802.1p 值的映射关系

设备内部优先级(服务等 级)	设备内部丢弃优先级(颜 色)	802.1p值
BE	green	0
BE	yellow	0
BE	red	0
AF1	green	1
AF1	yellow	1
AF1	red	1
AF2	green	2
AF2	yellow	2
AF2	red	2
AF3	green	3
AF3	yellow	3
AF3	red	3
AF4	green	4
AF4	yellow	4
AF4	red	4
EF	green	5
EF	yellow	5

设备内部优先级(服务等 级)	设备内部丢弃优先级(颜 色)	802.1p值
EF	red	5
CS6	green	6
CS6	yellow	6
CS6	red	6
CS7	green	7
CS7	yellow	7
CS7	red	7

IP报文从设备转发出去时,设备内部优先级/丢弃优先级与报文中DSCP值的缺省映射关系如表8-8所示。

表 8-8 出方向上设备内部优先级/丢弃优先级与 DSCP 值的映射关系

设备内部优先级(服务等 级)	设备内部丢弃优先级(颜 色)	DSCP值
BE	green	0
BE	yellow	0
BE	red	0
AF1	green	10
AF1	yellow	12
AF1	red	14
AF2	green	18
AF2	yellow	20
AF2	red	22
AF3	green	26
AF3	yellow	28
AF3	red	30
AF4	green	34
AF4	yellow	36
AF4	red	38
EF	green	46

设备内部优先级(服务等 级)	设备内部丢弃优先级(颜 色)	DSCP值
EF	yellow	46
EF	red	46
CS6	green	48
CS6	yellow	48
CS6	red	48
CS7	green	56
CS7	yellow	56
CS7	red	56

# 8.5 配置基于 DiffServ 域的优先级映射

### 背景信息

基于DiffServ域的优先级映射功能的配置逻辑如下:

- 1. 配置优先级信任模式:配置优先级信任模式可以确定设备根据哪种优先级进行映射。
- 2. 配置DiffServ域:配置DiffServ域可以确定外部优先级与内部优先级的映射关系。 以便设备根据内部优先级提供有差别的QoS服务。
- 3. 应用DiffServ域: 将DiffServ域应用在对象上,使DiffServ域中的映射和重标记关系生效。
- 4. 检查配置结果: 查看DiffServ域的配置信息。

# 8.5.1 配置优先级信任模式

# 背景信息

配置优先级信任模式可以确定设备根据哪种优先级进行映射。

### 操作步骤

步骤1 进入系统视图。

system-view

步骤2 进入接口视图。

**interface** *interface-type interface-number* 

步骤3 指定对报文按照某类优先级进行映射。

trust { 8021p { inner | outer } | dscp }

#### □ 说明

当以太接口为三层模式时,不能配置信任的优先级,默认信任报文中的DSCP值。 三层子接口不支持trust **8021p** inner命令。

#### ----结束

# 8.5.2 配置 DiffServ 域

### 背景信息

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

# 操作步骤

步骤1 进入系统视图。

system-view

步骤2 创建DiffServ域并进入DiffServ域视图。

diffserv domain ds-domain-name

default域定义了缺省情况下报文的外部优先级和内部优先级/丢弃优先级之间的映射关系。用户可以修改default域中定义的映射关系,但不能删除default域。

步骤3 请根据实际情况对设备的优先级映射进行定义。

操作	命令
在入方向,将VLAN报文的802.1p值映射 为内部优先级,并为报文着色	<b>8021p-inbound</b> <i>8021p-value</i> <b>phb</b> <i>service-class</i> [ <i>color</i> ]
在出方向,将内部优先级/丢弃优先级映 射为VLAN报文的802.1p值	8021p-outbound service-class color map 8021p-value
在入方向,将IP报文的DSCP值映射为内 部优先级,并为报文着色	ip-dscp-inbound dscp-value phb service-class [ color ]
在出方向,将内部优先级/丢弃优先级映 射为IP报文的DSCP值	ip-dscp-outbound service-class color map dscp-value

缺省优先级映射关系请参见8.4 优先级映射缺省配置。

#### ----结束

# 8.5.3 应用 DiffServ 域

#### 背景信息

当需要根据DiffServ域中定义的映射关系,对出/入设备的报文进行外部优先级到内部优先级/丢弃优先级之间的映射操作时,可以将DiffServ域绑定到报文的出/入接口,系统会根据DiffServ域中的映射关系进行报文外部优先级与内部优先级/丢弃优先级之间的映射。

### 操作步骤

步骤1 进入系统视图。

system-view

步骤2 进入接口视图。

interface interface-type interface-number

步骤3 应用DiffServ域。

trust upstream { ds-domain-name | none }

缺省情况下,接口上应用的是default域。

如果接口上配置了trust upstream none命令,系统对进入该接口的报文,不按照报文优先级映射。

#### □ 说明

设备不支持同时配置trust upstream none命令与qos phb marking 8021p disable、qos phb marking dscp enable命令。

步骤4 (可选)使能出方向报文的PHB与DSCP值的映射功能。

qos phb marking dscp enable

步骤5 (可选)去使能出方向报文的PHB与802.1p值的映射功能。

qos phb marking 8021p disable

----结束

# 8.5.4 检查配置结果

### 操作步骤

- 执行命令display diffserv domain [ brief | ds-domain-name ], 查看DiffServ域 的配置信息。
- 执行命令display qos queue statistics { interface interface-name | interface interface-type interface-number | slot slotid } , 查看基于队列的流量统计信息。
- 执行命令**display qos configuration interface** [ { *interface-type interface-number* | *interface-name* } ],查看接口上所有的QoS配置信息。

----结束

# 8.5.5 举例: 配置优先级映射

#### 组网需求

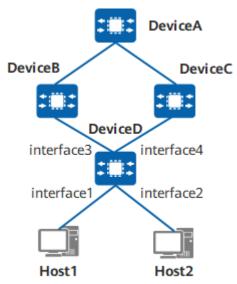
如<mark>图8-4</mark>所示,Host1和Host2通过DeviceD接入DeviceB和DeviceC,再经由DeviceA访问网络。

Host1和Host2的报文802.1p值均为0,用户希望对Host1和Host2进行差分服务,使 Host1的服务等级高于Host2,从而保证Host1业务的低延时需求。

#### 图 8-4 优先级映射配置组网图

#### □ 说明

本例中interface1,interface2,interface3,interface4分别代表10GE1/0/1,10GE1/0/2,10GE1/0/3和10GE1/0/4。



# 操作步骤

步骤1 创建VLAN并配置各接口,实现DeviceD与Host1、Host2、DeviceB、DeviceC之间的互通。

# 创建VLAN 100、200。

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

# 配置DeviceD上接口10GE1/0/3、10GE1/0/4的接入类型为Trunk,并将接口 10GE1/0/1加入VLAN 100、10GE1/0/2加入VLAN 200,接口10GE1/0/3、10GE1/0/4 加入VLAN 100和VLAN 200。仅S6730-H-V2系列、S5732-H-V2系列、S5755-H系列 支持命令**portswitch**。

```
[DeviceD] interface 10ge 1/0/1
[DeviceD-10GE1/0/1] portswitch
[DeviceD-10GE1/0/1] port default vlan 100
[DeviceD-10GE1/0/1] quit
[DeviceD] interface 10ge 1/0/2
[DeviceD-10GE1/0/2] portswitch
[DeviceD-10GE1/0/2] port default vlan 200
[DeviceD-10GE1/0/2] quit
[DeviceD] interface 10ge 1/0/3
[DeviceD-10GE1/0/3] portswitch
[DeviceD-10GE1/0/3] port link-type trunk
[DeviceD-10GE1/0/3] port trunk allow-pass vlan 100 200
[DeviceD-10GE1/0/3] quit
[DeviceD] interface 10ge 1/0/4
[DeviceD-10GE1/0/4] portswitch
[DeviceD-10GE1/0/4] port link-type trunk
[DeviceD-10GE1/0/4] port trunk allow-pass vlan 100 200
[DeviceD-10GE1/0/4] quit
```

步骤2 配置接口信任的外部优先级为外层802.1p值。

# 配置接口10GE1/0/1、10GE1/0/2、10GE1/0/3、10GE1/0/4信任外层802.1p值。缺省情况下,二层接口信任外层802.1p值,此配置步骤可省略。

```
[DeviceD] interface 10ge 1/0/1
[DeviceD-10GE1/0/1] trust 8021p outer
[DeviceD-10GE1/0/1] quit
[DeviceD] interface 10ge 1/0/2
[DeviceD-10GE1/0/2] trust 8021p outer
[DeviceD-10GE1/0/2] quit
[DeviceD] interface 10ge 1/0/3
[DeviceD-10GE1/0/3] trust 8021p outer
[DeviceD-10GE1/0/3] quit
[DeviceD] interface 10ge 1/0/4
[DeviceD] interface 10ge 1/0/4
[DeviceD-10GE1/0/4] trust 8021p outer
[DeviceD-10GE1/0/4] quit
```

#### 步骤3 创建并配置DiffServ域,再将DiffServ域绑定到接口上。

# 在DeviceD上创建DiffServ域ds1、ds2,并配置将来自Host1和Host2的报文的802.1p 值映射到内部优先级。

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

# 将DiffServ域ds1和ds2分别绑定到接口10GE1/0/1、10GE1/0/2。

```
[DeviceD] interface 10ge 1/0/1
[DeviceD-10GE1/0/1] trust upstream ds1
[DeviceD-10GE1/0/1] quit
[DeviceD] interface 10ge 1/0/2
[DeviceD-10GE1/0/2] trust upstream ds2
[DeviceD-10GE1/0/2] quit
```

#### ----结束

# 检查配置结果

# 查看出接口队列统计信息。内部优先级AF2对应的队列2和内部优先级AF4对应的队列4上有报文统计信息,说明优先级映射配置成功。

#### 配置脚本

#### DeviceD的配置脚本

```
# sysname DeviceD
# vlan batch 100 200
# diffserv domain ds1
8021p-inbound 0 phb af4 green
# diffserv domain ds2
8021p-inbound 0 phb af2 green
# interface 10GE1/0/1
port default vlan 100
trust upstream ds1
# interface 10GE1/0/2
port default vlan 200
trust upstream ds2
```

```
#
interface 10GE1/0/3
port link-type trunk
port trunk allow-pass vlan 100 200
#
interface 10GE1/0/4
port link-type trunk
port trunk allow-pass vlan 100 200
#
return
```

# 8.6 配置端口优先级

### 背景信息

在以下情况中,设备根据端口优先级对报文进行后续的差分服务:

- 接口下配置了trust upstream none命令。
- 接口收到了不带VLAN Tag的报文。

#### □ 说明

- Eth-Trunk成员接口不支持配置端口优先级。
- 如果入接口不应用DiffServ域且同时配置了端口优先级,则进入设备的报文被打上 VLAN Tag,并添加端口优先级为外部优先级,且按照端口优先级入队列。
- 当以太网接口为三层模式时,不能配置端口优先级值,端口优先级值为0。

#### 操作步骤

步骤1 进入系统视图。

system-view

步骤2 进入接口视图。

interface interface-type interface-number

步骤3 配置端口优先级。

port priority priority-value

----结束

# 8.7 配置本设备发送的协议报文的内部优先级

#### 背景信息

报文在设备中是按照内部优先级进行处理的。用户可以通过修改本设备所发送的协议报文的内部优先级,以确保内部优先级高的协议报文在本设备得到优先处理。

#### 操作步骤

步骤1 进入系统视图。

system-view

步骤2 配置本设备发送的协议报文的内部优先级。

set priority traffic-class traffic-class-value

缺省情况下,未配置本设备发送的协议报文的内部优先级,所有协议报文在本设备中 按照其原定的内部优先级进行发送。

----结束

# 8.8 配置内部优先级与队列的映射关系

# 背景信息

由于设备是基于队列对报文进行调度,因此将报文的外部优先级映射为内部优先级 (PHB行为)后,还需要根据内部优先级与队列的映射关系将报文送进对应的队列进 行调度,以实现对报文的差分服务。

缺省情况下,内部优先级与端口队列的对应关系是一对一。在实际部署时,有时需要两类或多类不同的内部优先级放入同一个队列中进行调度,从而有效地节约设备缓存。设备按照内部优先级将报文送入不同的端口队列,从而针对队列进行流量整形、拥塞避免、队列调度等处理。

#### 山 说明

仅S6730-H-V2、S5732-H-V2和S5755-H系列支持该功能。

#### 操作步骤

步骤1 进入系统视图。

system-view

步骤2 配置内部优先级和队列之间的映射关系。

qos local-precedence-queue-map service-class queue-index

缺省情况下内部优先级与队列索引关系请参见8.4 优先级映射缺省配置。

----结束

# 8.9 配置报文的优先级

#### 操作步骤

步骤1 进入系统视图。

system-view

步骤2 配置报文的802.1p值。

set priority 8021p 8021p-value

缺省情况下,未配置报文的802.1p值。

步骤3 配置报文的DSCP值。

set priority dscp dscp-value

缺省情况下,未配置报文的DSCP值。

----结束

# 8.10 优先级映射常见配置错误

# 8.10.1 报文未进入正确队列

### 故障现象

报文未进入正确队列。

### 可能原因

报文未进入正确队列的常见原因主要包括:

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

### 操作步骤

#### 步骤1 检查优先级映射关系是否正确

进入报文入方向的接口视图,执行命令display this,查看入接口配置的trust upstream命令(如果没有配置,系统缺省信任default域),然后执行命令display diffserv domain ds-domain-name检查DiffServ域中配置的优先级映射关系是否与业务规划符合:

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

#### 步骤2 检查入接口上是否有影响报文入队列的配置

如果入接口上配置了:

- 入方向且与报文匹配的traffic-policy,若流策略下配置了remark local-precedence动作,系统按照remark后的内部优先级入队列。
- trust upstream none,则进入该接口的所有报文不进行优先级映射,报文按照端口优先级入队列。

检查入接口是否有上述影响报文入队列的配置:

- 如果有,请根据以上情况删除或修改该配置。
- 如果没有,执行步骤3。

#### 步骤3 检查报文所属VLAN下是否有影响报文入队列的配置

如果报文所属VLAN下配置了:

• 入方向且与报文匹配的traffic-policy,若流策略下配置了remark local-precedence动作,系统按照remark后的内部优先级入队列。

● 入方向且与报文匹配的traffic-policy,若流策略下有remark 8021p动作,则系统根据remark后的优先级进行外部优先级到内部优先级的映射,并根据映射后的内部优先级入队列。

检查报文所属VLAN下是否有上述影响报文入队列的配置:

- 如果有,请根据以上情况删除或修改该配置。
- 如果没有,执行步骤4。

#### 步骤4 检查全局是否有影响报文入队列的配置

#### 如果全局配置了:

- qos local-precedence-queue-map,则系统按照此命令指定的内部优先级与队列之间的映射关系入队列。
- 入方向且与报文匹配的traffic-policy global,若流策略下配置了remark local-precedence动作,系统按照remark后的内部优先级入队列。
- 入方向且与报文匹配的traffic-policy global,若流策略下有remark 8021p动作,则系统根据remark后的优先级进行外部优先级到内部优先级的映射,并根据映射后的内部优先级入队列。

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

----结束

# 8.10.2 优先级映射结果不正确

#### 故障现象

优先级映射结果不正确。

#### 可能原因

优先级映射结果不正确的常见原因主要包括:

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

#### 操作步骤

#### **步骤1** 检查报文在出接口是否进入正确的队列

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

- 如果报文在出接口没有按照要求入队列,请参见**8.10.1 报文未进入正确队列**定位错误。
- 如果报文在出接口进入了正确的队列,执行步骤2。

步骤2 检查出/入接口信任的优先级类型是否正确

进入出/入接口视图,执行命令display this,查看接口配置的trust命令,看信任的优先级类型是否与业务规划符合:

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

#### 步骤3 检查出/入接口信任的DiffServ域中的优先级映射关系是否正确

进入出/入接口视图,执行命令display this,查看出/入接口配置的trust upstream命令。

然后执行命令**display diffserv domain** *ds-domain-name*,检查内部优先级/丢弃优先级和外部优先级之间的映射是否与业务规划符合:

- 如果不符合,执行命令ip-dscp-outbound或8021p-outbound正确配置内部优先级/丢弃优先级到外部优先级的映射。
- 如果符合,执行步骤4。

#### 步骤4 检查出/入接口是否有影响优先级映射的配置

#### 如果接口下:

- 没有配置qos phb marking dscp enable,则系统对接口出方向的报文不进行 PHB与DSCP值的映射。
- 配置了**qos phb marking 8021p disable**,则系统对接口出方向的报文不进行 PHB与802.1p值的映射。
- 配置了trust upstream none,则系统对从此接口出去的报文不进行优先级映射。
- 出/入方向且与报文匹配的traffic-policy,若流策略下有remark 8021p或remark dscp动作,报文优先级为remark后的外部优先级。

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

#### ----结束

# **9** 流量监管、流量整形和接口限速配置

- 9.1 流量监管、流量整形和接口限速简介
- 9.2 流量监管、流量整形和接口限速原理描述
- 9.3 流量监管配置注意事项
- 9.4 流量整形配置注意事项
- 9.5 接口限速配置注意事项
- 9.6 流量监管、流量整形和接口限速缺省配置
- 9.7 配置流量监管
- 9.8 配置流量整形
- 9.9 配置接口限速
- 9.10 配置QoS模板
- 9.11 维护流量监管、流量整形和接口限速

# 9.1 流量监管、流量整形和接口限速简介

### 定义

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

- 流量监管TP(Traffic Policing)是监督不同流量进入网络的速率,对超出部分的流量进行"惩罚",使进入的流量被限制在一个合理的范围之内,从而保护网络资源和用户的利益。
- 流量整形TS(Traffic Shaping)是一种主动调整流量输出速率的措施,将上游不规整的流量进行削峰填谷,使流量输出比较平稳,从而解决下游设备的拥塞问题。
- 接口限速LR(Line Rate)是对一个接口上发送或者接收全部报文的总速率进行限制。当不需要区分报文类型而要限制通过接口全部流量速率时,通过接口限速功能可以简化配置。

#### 目的

当上游设备报文的发送速率大于下游设备接收速率,或者下游设备的接口速率小于上游设备的接口速率时,可能会引起网络的拥塞。如果不限制用户发送的业务流量大小,大量用户不断突发的业务数据会使网络更加拥挤。为了使有限的网络资源更有效的为用户服务,需要对用户的业务流量加以限制。流量监管、流量整形和接口限速通过监督进入网络的流量速率,以达到限制流量,提高网络资源使用效率的目的,从而保证更好的为用户提供服务。

# 9.2 流量监管、流量整形和接口限速原理描述

# 9.2.1 流量评估与令牌桶技术

#### 概述

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

令牌桶可以看作是一个存放一定数量令牌的容器。系统按设定的速度向桶中放置令牌,当桶中令牌满时,多出的令牌溢出,桶中令牌不再增加。在使用令牌桶对流量规格进行评估时,是以令牌桶中的令牌数量是否足够满足报文的转发为依据的。如果桶中存在足够的令牌可以用来转发报文,称流量遵守或符合约定值,否则称为不符合或超标。

关于令牌桶处理报文的方式,RFC中定义了以下标记算法:

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

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

### 单速双桶

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

如<mark>图9-1</mark>所示,为方便描述将两个令牌桶称为C桶和E桶,用Tc和Te表示桶中的令牌数量。单速双桶有3个参数:

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

#### 系统按照CIR速率向桶中投放令牌:

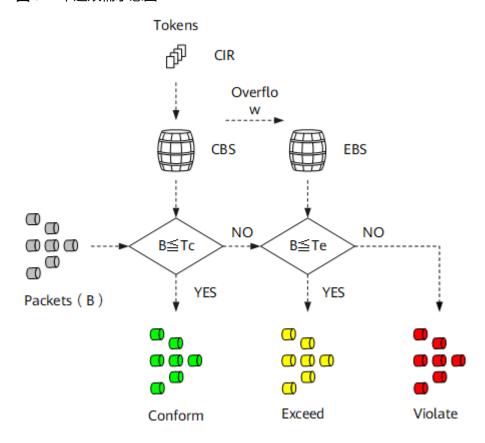
- 若Tc<CBS, Tc增加;
- 若Tc=CBS, Te<EBS, Te增加;
- 若Tc=CBS, Te=EBS,则都不增加。

#### 对于到达的报文,用B表示报文的大小:

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

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

图 9-1 单速双桶示意图



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

#### □ 说明

为方便计算,此处1Mbit/s按1×10<sup>6</sup>bit/s计算。

假设第1个到达的报文是1500bytes。检查C桶发现令牌数大于数据包的长度,所以数据包被标为绿色、C桶减少令牌1500bytes,还剩500bytes,E桶令牌数量保持不变。

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

报文处理过程汇总见表9-1。

表 9-1 单速双桶模式下报文处理过程

包序	时刻 (ms)	报文 长度 (byte s)	与上 次加令 牌的 间隔 (ms)	本轮 增加 令牌 (byte s)	令牌增加后各 桶令牌(bytes)		报文处理后各 桶剩余令牌 (bytes)		报文标记
号					C桶	E桶	C桶	E桶	结果
-	-	-	-	-	2000	2000	2000	2000	-
1	0	1500	0	0	2000	2000	500	2000	绿色
2	1	1500	1	125	625	2000	625	500	黄色
3	2	1000	1	125	750	500	750	500	红色
4	22	1500	20	2500	2000	1750	500	1750	绿色

# 单速单桶

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

如<mark>图9-2</mark>所示,为方便描述将此令牌桶称为C桶,用Tc表示桶中的令牌数量。单速单桶有2个参数:

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

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

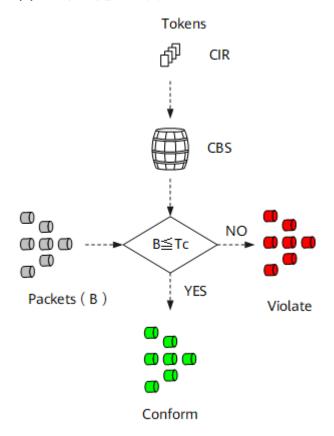
对于到达的报文,用B表示报文的大小:

● 若B≤Tc,报文被标记为绿色,且Tc减少B;

• 若B>Tc,报文被标记为红色,Tc不减少。

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

图 9-2 单速单桶示意图



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

#### □ 说明

为方便计算,此处1Mbit/s按1×10<sup>6</sup>bit/s计算。

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

报文处理过程汇总见表9-2。

表 9-2 单速单桶模式下报文处理过程

包序号	时刻 (ms)	报文长 度 (bytes)	与上次 添加令 牌的间 隔(ms)	本轮增 加令牌 (bytes)	令牌增 加后C桶 令牌 (bytes)	报文处 理后C桶 剩余令 牌 (bytes)	报文标 记结果
-	-	-	-	-	2000	2000	-
1	0	1500	0	0	2000	500	绿色
2	1	1500	1	125	625	625	红色
3	2	1000	1	125	750	750	红色
4	22	1500	20	2500	2000	500	绿色

### 双速双桶

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

如<mark>图9-3</mark>所示,为方便描述将两个令牌桶称为P桶和C桶,用Tp和Tc表示桶中的令牌数量。双速双桶有4个参数:

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

系统按照PIR速率向P桶中投放令牌,按照CIR速率向C桶中投放令牌:

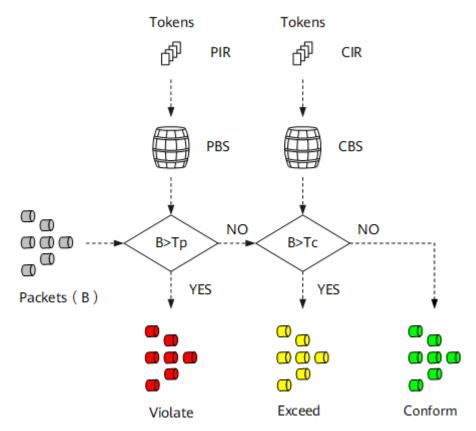
- 当Tp<PBS时,P桶中令牌数增加,否则不增加。
- 当Tc<CBS时,C桶中令牌数增加,否则不增加。

对于到达的报文,用B表示报文的大小:

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

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

图 9-3 双速双桶示意图



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

#### □ 说明

为方便计算,此处1Mbit/s按1×10<sup>6</sup>bit/s计算。

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

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

报文处理过程汇总见表9-3。

表 9-3 双速双桶模式下报文处理过程

包序	报文	长度	加令	本轮增加令 牌(bytes)		令牌增加后 各桶令牌 (bytes)		报文处理后 各桶剩余令 牌(bytes)		报文标记
号	(ms)	(byt es)	牌的 间隔 (ms)	C桶	P桶	C桶	P桶	C桶	P桶	结果
-	-	-	-	-	-	2000	3000	2000	3000	-
1	0	1500	0	0	0	2000	3000	500	1500	绿色
2	1	1800	1	125	250	625	1750	625	1750	红色
3	2	1000	1	125	250	750	2000	750	1000	黄色
4	22	1500	20	2500	5000	2000	3000	500	1500	绿色

## 三种令牌桶模式的区别和应用

三种令牌桶模式之间的区别和相互关系如表9-4所示。

表 9-4 三种令牌桶模式之间的区别和相互关系

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

区别	单速单桶	单速双桶	双速双桶
相互关系	单速双桶模式中,如   的。	果EBS等于0,其效果	和单速单桶是一样
	双速双桶模式中,如 的。	果PIR等于CIR,其效5	<b>果和单速单桶是一样</b>

基于上述三种令牌桶模式之间的区别,其功能和选用场景也有所不同,见表9-5。

表 9-5 三种令牌桶模式的功能及选用场景

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

## 色敏模式

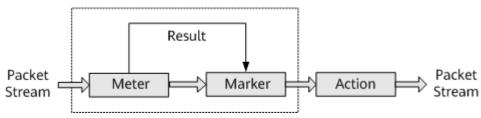
色敏模式下,如果到达的报文本身已经被标记为红、黄或者绿等颜色,令牌桶对流量的评估会参考报文已标记颜色,即报文本身已携带颜色会影响令牌桶的评估结果,评估机制简单的来说遵循以下原则:

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

## 9.2.2 流量监管

流量监管可以对不同流量进行监督,对超出部分的流量进行"惩罚",使进入的流量被限制在一个合理的范围之内,从而保护网络资源和企业网用户的利益。

图 9-4 流量监管组件



如图9-4所示,流量监管由三部分组成:

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

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

## 9.2.3 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。

下面以采用单速单桶技术的基于流的队列整形为例介绍流量整形的处理流程,其处理 流程如图9-5所示。

队列 不需要进行 报文流 队列整形的报文 报文流 000 തതത 按规定的速率 0000 യയയ 向桶中存放令牌 需要进行 000000队列整形的报文 符合速率限制  $\mathbf{o}$ 流分类 的报文 令牌桶 0000 

超过速率限制: 的报文

0000

ത ത

缓存队列已满时

丟弃的报文

缓存队列

图 9-5 流量整形处理流程图

#### 具体处理流程如下:

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。

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

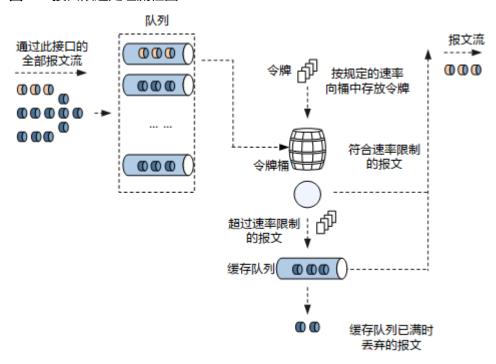
## 9.2.4 接口限速

接口限速可以限制一个接口上发送或者接收报文的总速率。

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

接口限速支持出/入两个方向,下面以接口下采用单速单桶技术为例介绍出方向接口限速的处理流程,其处理流程如图9-6所示。

#### 图 9-6 接口限速处理流程图



#### 具体处理流程如下:

- 1. 如果令牌桶中有足够的令牌可以用来发送报文,则报文直接被发送,在报文被发送的同时,令牌做相应的减少。
- 2. 如果令牌桶中没有足够的令牌,则将报文放入缓存队列,如果报文放入缓存队列时,缓存队列已满,则丢弃报文。

3. 缓存队列中有报文的时候,会与令牌桶中的令牌数作比较,如果令牌数足够发送报文则转发报文,直到缓存队列中的报文全部发送完毕为止。

# 9.3 流量监管配置注意事项

## License 依赖

流量监管无需License许可即可使用。

## 硬件依赖

表 9-6 支持本特性的硬件

系列	支持产品
S5735-L-V2 series	S5735-L10T4X-A-V2/S5735-L14P2S-QA-V2/S5735-L16LP2UM2X-QA-V2/S5735-L16LP2X-QA-V2/S5735-L16LP2X-QA-V2/S5735-L16P2UM2X-QA-V2/S5735-L16T4S-A-V2/S5735-L16T4X-QA-V2/S5735-L24P4S-A-V2/S5735-L24P4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L48LP4S-A-V2/S5735-L48LP4XE-A-V2/S5735-L48P4XE-A-V2/S5735-L48S4XE-A-V2/S5735-L48S4XE-A-V2/S5735-L48T4S-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L8P4X-A-V2/S5735-L8P4X-A-V2/S5735-L8P4X-A-V2/S5735-L8P4X-QA-V2/S5735-L8P4X-A-V2/S5735-L8P4X-QA-V2/S5735-L8P4X-QA-V2/S5735-L8T4X-QA-V2
S5735-S-V2 series	S5735-S24HS4XE-V2/S5735-S24P4XE-V2/S5735- S24ST4XE-V2/S5735-S24T4XE-V2/S5735- S24U4XE-V2/S5735-S48HS4XE-V2/S5735- S48P4XE-V2/S5735-S48S4XE-V2/S5735-S48T4XE- V2/S5735-S48U4XE-V2
S5735I-L-V2 series	S5735I-L10T4X-A-V2/S5735I-L8P4X-A-V2
S5755-H series	S5755-H24N4Y-A/S5755-H24P4Y2CZ/S5755- H24T4Y2CZ/S5755-H24U4Y2CZ/S5755- H24UN4Y2CZ/S5755-H24UTM4X4Y2C/S5755- H48N4Y-A/S5755-H48P4Y2CZ/S5755-H48T4Y2CZ/ S5755-H48U4Y2CZ/S5755-H48UN4Y2CZ/S5755- H48UTM4X4Y2C
S6730-H-V2 series	S6730-H24X6C-V2/S6730-H28X6CZ-V2/S6730- H48X6C-V2/S6730-H48X6CZ-V2/S6730-H48Y6C- V2
S5732-H-V2 series	S5732-H24S4X6QZ-V2/S5732-H24UM4Y2CZ-KV2/ S5732-H24UM4Y2CZ-V2/S5732-H44S4X6QZ-V2/ S5732-H48UM4Y2CZ-KV2/S5732-H48UM4Y2CZ- V2

系列	支持产品
S5735I-H-V2 series	S5735I-H8T4S2XN-V2
S5735I-S-V2 series	S5735I-S24T4XE-V2/S5735I-S24U4XE-V2/S5735I- S8T4SN-V2/S5735I-S8T4XN-V2/S5735I-S8U4XN- V2

## 特性限制

无

# 9.4 流量整形配置注意事项

## License 依赖

流量整形无需License许可即可使用。

## 硬件依赖

表 9-7 支持本特性的硬件

系列	支持产品
S5735-L-V2 series	S5735-L10T4X-A-V2/S5735-L14P2S-QA-V2/S5735-L16LP2UM2X-QA-V2/S5735-L16LP2X-QA-V2/S5735-L16LP2UM2X-QA-V2/S5735-L16T4S-A-V2/S5735-L16T4X-QA-V2/S5735-L24P4XE-A-V2/S5735-L24P4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L48LP4XE-A-V2/S5735-L48LP4XE-A-V2/S5735-L48P4XE-A-V2/S5735-L48S4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L8P4X-A-V2/S5735-L8P4X-A-V2/S5735-L8P4X-A-V2/S5735-L8P4X-A-V2/S5735-L8P4X-A-V2/S5735-L8P4X-A-V2/S5735-L8P4X-QA-V2/S5735-L8T4X-QA-V2
S5735-S-V2 series	S5735-S24HS4XE-V2/S5735-S24P4XE-V2/S5735- S24ST4XE-V2/S5735-S24T4XE-V2/S5735- S24U4XE-V2/S5735-S48HS4XE-V2/S5735- S48P4XE-V2/S5735-S48S4XE-V2/S5735-S48T4XE- V2/S5735-S48U4XE-V2
S5735I-L-V2 series	S5735I-L10T4X-A-V2/S5735I-L8P4X-A-V2

系列	支持产品	
S5755-H series	S5755-H24N4Y-A/S5755-H24P4Y2CZ/S5755- H24T4Y2CZ/S5755-H24U4Y2CZ/S5755- H24UN4Y2CZ/S5755-H24UTM4X4Y2C/S5755- H48N4Y-A/S5755-H48P4Y2CZ/S5755-H48T4Y2CZ S5755-H48U4Y2CZ/S5755-H48UN4Y2CZ/S5755- H48UTM4X4Y2C	
S6730-H-V2 series	S6730-H24X6C-V2/S6730-H28X6CZ-V2/S6730- H48X6C-V2/S6730-H48X6CZ-V2/S6730-H48Y6C- V2	
S5732-H-V2 series	S5732-H24S4X6QZ-V2/S5732-H24UM4Y2CZ-KV2/ S5732-H24UM4Y2CZ-V2/S5732-H44S4X6QZ-V2/ S5732-H48UM4Y2CZ-KV2/S5732-H48UM4Y2CZ- V2	
S5735I-H-V2 series	S5735I-H8T4S2XN-V2	
S5735I-S-V2 series	S5735I-S24T4XE-V2/S5735I-S24U4XE-V2/S5735I- S8T4SN-V2/S5735I-S8T4XN-V2/S5735I-S8U4XN- V2	

## 特性限制

表 9-8 本特性的使用限制

特性限制	系列	涉及产品
对于S5735-S-V2 Series/S5735-L-V2 Series/ S5735I-L-V2 Series/S5735I-S-V2 Series/S5735I-H-V2 Series: 出方向使用64个car模拟64个队列的整形,超出的队列整形可能出现调度不准的缺陷。	S5735-S- V2 series S5735-L- V2 series S5735I-S- V2 series S5735I-H- V2 series	S5735-S24HS4XE-V2/S5735-S24P4XE-V2/S5735-S24ST4XE-V2/S5735-S24T4XE-V2/S5735-S24U4XE-V2/S5735-S48HS4XE-V2/S5735-S48S4XE-V2/S5735-S48U4XE-S4-V2/S5735-S48U4XE-S4-V2/S5735-S48U4XE-S4-V2/S5735-S48U4XE-S4-V2/S5735-S48U4XE-S4-V2/S5735-S48U4XE-S4-V2/S5735-S48U4XE-S4-V2/S5735-S48U4XE-S4-V2/S5735-S48U4XE-S4-V2/S5735-S48U4XE-S4-V2/S5735-S48U4XE-S4-V2/S5735-S48U4XE-S4-V2/S5735-S48U4XE-S4-V2/S5735-S5735-S5-S5735-S5-S5735-S5-S5735-S5735-S5-S5735-S5-S5735-S5-S5735-S5-S5735-S5-S5735-S5-S5735-S5-S5-S5735-S5-S5735-S5-S5735-S5-S5735-S5-S5735-S5-S5735-S5-S5735-S5-S5735-S5-S5735-S5-S5-S5735-S5-S5735-S5-S5-S5735-S5-S5-S5735-S5735-S5-S5735-S5735-S5735-S5735-S5-S5735-S5-S5735-S5-S5735-S5-S5735-S5-S5735-S5-S5735-S5-S5735-S5-S5735-S5-S5735-S5-S5735-S5-S5735-S5-S5735-S5-S5735-S5-S5735-S5-S5735-S5-S5-S5735-S5-S5-S5735-S5-S5735-S5-S5735-S5-S5735-S5-S5-S5-S5735-S5-S5-S5-S5-S5-S55-S5-S5-S55-S5-S55-S5-S

特性限制	系列	涉及产品
		L48T4XE-A-V2/ S5735-L48T4XE- D-V2/S5735- L8P2T4X-A-V2/ S5735-L8P4S-A- V2/S5735-L8P4X- QA-V2/S5735- L8T4S-A-V2/ S5735-L8T4X-QA- V2
		S5735I-L10T4X-A- V2/S5735I-L8P4X- A-V2
		S5735I-S24T4XE- V2/S5735I- S24U4XE-V2/ S5735I-S8T4SN- V2/S5735I- S8T4XN-V2/ S5735I-S8U4XN- V2
		S5735I- H8T4S2XN-V2

# 9.5 接口限速配置注意事项

## License 依赖

接口限速无需License许可即可使用。

## 硬件依赖

表 9-9 支持本特性的硬件

系列	支持产品
S5735-L-V2 series	S5735-L10T4X-A-V2/S5735-L14P2S-QA-V2/S5735-L16LP2UM2X-QA-V2/S5735-L16LP2X-QA-V2/S5735-L16P2UM2X-QA-V2/S5735-L16T4S-A-V2/S5735-L16T4X-QA-V2/S5735-L24P4S-A-V2/S5735-L24P4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L48LP4S-A-V2/S5735-L48LP4XE-A-V2/S5735-L48P4XE-A-V2/S5735-L48S4XE-A-V2/S5735-L48T4S-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L8P4X-A-V2/S5735-L8P4X-A-V2/S5735-L8P4X-A-V2/S5735-L8P4X-QA-V2/S5735-L8P4X-QA-V2/S5735-L8P4X-QA-V2/S5735-L8P4X-QA-V2/S5735-L8T4X-QA-V2
S5735-S-V2 series	S5735-S24HS4XE-V2/S5735-S24P4XE-V2/S5735- S24ST4XE-V2/S5735-S24T4XE-V2/S5735- S24U4XE-V2/S5735-S48HS4XE-V2/S5735- S48P4XE-V2/S5735-S48S4XE-V2/S5735-S48T4XE- V2/S5735-S48U4XE-V2
S5735I-L-V2 series	S5735I-L10T4X-A-V2/S5735I-L8P4X-A-V2
S5755-H series	S5755-H24N4Y-A/S5755-H24P4Y2CZ/S5755- H24T4Y2CZ/S5755-H24U4Y2CZ/S5755- H24UN4Y2CZ/S5755-H24UTM4X4Y2C/S5755- H48N4Y-A/S5755-H48P4Y2CZ/S5755-H48T4Y2CZ/ S5755-H48U4Y2CZ/S5755-H48UN4Y2CZ/S5755- H48UTM4X4Y2C
S6730-H-V2 series	S6730-H24X6C-V2/S6730-H28X6CZ-V2/S6730- H48X6C-V2/S6730-H48X6CZ-V2/S6730-H48Y6C- V2
S5732-H-V2 series	S5732-H24S4X6QZ-V2/S5732-H24UM4Y2CZ-KV2/ S5732-H24UM4Y2CZ-V2/S5732-H44S4X6QZ-V2/ S5732-H48UM4Y2CZ-KV2/S5732-H48UM4Y2CZ- V2
S5735I-H-V2 series	S5735I-H8T4S2XN-V2
S5735I-S-V2 series	S5735I-S24T4XE-V2/S5735I-S24U4XE-V2/S5735I- S8T4SN-V2/S5735I-S8T4XN-V2/S5735I-S8U4XN- V2

## 特性限制

无

## 9.6 流量监管、流量整形和接口限速缺省配置

流量监管、流量整形和接口限速的主要缺省配置如表9-10所示。

表 9-10 流量监管、流量整形和接口限速的缺省配置

参数	缺省配置
一级CAR的流量监管(MQC方式)	未启用
流分类下各规则之间的逻辑运算符	or
队列流量整形	未启用
队列流量整形参数	接口的最大带宽
流量监管实现接口限速	未启用
流量整形实现接口限速	未启用
流量整形实现接口限速的整形速率	接口的最大带宽
管理网口的流量限速	3000pps

## 9.7 配置流量监管

## 9.7.1 配置一级 CAR 的流量监管 (MQC 方式)

## 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,可以配置一级CAR的流量监管,即MQC方式实现流量监管。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。

在端口上同时应用QoS CAR和MQC的流量统计时,QoS CAR的报文统计信息仅包含未被MQC流策略命中的报文。

设备对同一个芯片资源上的接口统一做car,对不同芯片资源上的接口分别做car。因此,当包含流量监管的流策略应用在Eth-Trunk接口、全局或VLAN时,如果应用对象包含的接口属于N个芯片资源,则实际限速为car的N倍。

比如,假设interface1、interface2属于芯片资源0,interface3、interface4属于芯片资源1。若将interface1、interface2、interface3、interface4加入VLAN10,并在VLAN10上应用了限速1Mbit/s的流策略,实际上interface1和interface2限速了1Mbit/s,interface3和interface4限速了1Mbit/s,即VLAN10上应用了该流策略后,实际限速为2Mbit/s。

## 操作步骤

#### 步骤1 配置流分类。

流分类的配置方式,请参考MQC配置中的3.4 配置流分类。

#### 步骤2 配置流行为。

1. (可选)配置计算流量监管的速率时不包括报文的帧间隙和前导码。

gos car ifg disable

2. 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。

traffic behavior behavior-name

3. 配置CAR动作。

car cir cir-value [ kbps | mbps | gbps ] [ pir pir-value [ kbps | mbps | gbps ] ] [ cbs cbs-value [ bytes | kbytes | mbytes ] pbs pbs-value [ bytes | kbytes | mbytes ] ] [ share ] [ mode { color-blind | color-aware } ] [ green pass [ service-class class color color-value ] | yellow { discard | pass [ service-class class color color-value ] } | red { discard | pass [ service-class class color color-value ] } ] \*

4. 退出流行为视图。

quit

#### 步骤3 配置流策略。

1. 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。

traffic policy policy-name

2. 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。

classifier classifier-name behavior behavior-name [ precedence precedence-value ]

3. 退出流策略视图。

quit

#### 步骤4 应用流策略。

- 在全局上应用流策略。
  - a. 在全局上应用流策略。 traffic-policy *policy-name* global [ slot *slot-id* ] { inbound | outbound }
- 在接口上应用流策略。
  - a. 进入接口视图。

interface interface-type interface-number

b. 在接口上应用流策略。

traffic-policy policy-name { inbound | outbound }

c. 退出接口视图。

quit

- 在VLAN上应用流策略。
  - a. 创建VLAN,并进入VLAN视图。

vlan vlan-id

b. 在VLAN上应用流策略。

traffic-policy policy-name { inbound | outbound }

应用后,系统对属于该VLAN并匹配流分类中规则的入方向或出方向报文实施 策略控制。

c. 退出VLAN视图。

quit

#### ----结束

## 9.7.2 配置二级 CAR 的流量监管

### 前提条件

已经配置一级CAR的流量监管,具体步骤请参见9.7.1 配置一级CAR的流量监管(MQC方式)。

## 背景信息

设备支持二级CAR的流量监管,即系统对满足流分类规则的业务流通过MQC实现流量监管(一级CAR)后,可以将同一流策略中满足一级CAR的流分类的所有业务流聚合在一起再做一次流量监管(二级CAR)。二级CAR的流量监管可以实现用户流量的统计复用和精细业务的控制。

### 操作步骤

步骤1 进入系统视图。

system-view

步骤2 (可选)配置计算流量监管的速率时不包括报文的帧间隙和前导码。

qos car ifg disable

#### 步骤3 配置CAR模板。

qos car car-name { percent percent-value | cir cir-value [ kbps | mbps | gbps ] [ cbs cbs-value [ bytes | kbytes | mbytes ] [ pbs pbs-value [ bytes | kbytes | mbytes ] ] | pir pir-value [ kbps | mbps | gbps ] [ cbs cbs-value [ bytes | kbytes | mbytes ] pbs pbs-value [ bytes | kbytes | mbytes ] ] ] }

#### 山 说明

该QoS CAR模板的CIR必须大于一级CAR的流行为中配置的CAR的CIR。

#### 步骤4 配置共享CAR动作。

#### □ 说明

仅S6730-H-V2、S5732-H-V2和S5755-H系列支持共享CAR动作。

1. 进入流行为视图。

traffic behavior behavior-name

2. 配置共享CAR动作。

car car-name share

----结束

## 9.7.3 检查配置结果

#### 操作步骤

操作	命令
查看已配置的流分类信息	display traffic classifier [ classifier- name ]

操作	命令
查看已配置的流行为信息	display traffic behavior [ behavior- name ]
查看已配置的流策略信息	display traffic policy [ policy-name [ classifier classifier-name ] ]
查看流策略的应用记录	display traffic-policy applied-record [ policy-name ]
查看基于一级CAR的流量监管(MQC方式)配置的流量统计信息	display traffic-policy statistics
查看CAR模板的配置信息	display qos car [ car-name ]

# 9.7.4 举例: 配置一级 CAR 的流量监管 (MQC 方式)

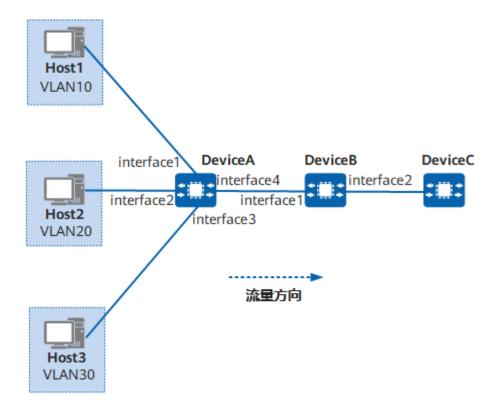
## 组网需求

如<mark>图9-7</mark>所示,Host1、Host2和Host3通过DeviceA和DeviceB上送报文,经DeviceC与外部网络互通。把连接Host1的接口划分到VLAN 10,把连接Host2的接口划分到VLAN 20,把连接Host3的接口划分到VLAN 30。

#### 图 9-7 MQC 实现流量监管配置组网图

## □ 说明

本例中interface1、interface2、interface3、interface4分别代表10GE1/0/1、10GE1/0/2、10GE1/0/3、10GE1/0/4。



根据每个租户的业务量,在DeviceB上需要对不同Host的报文分别进行流量监管,以将流量限制在一个合理的范围之内,具体带宽需求如表9-11所示。

表 9-11 DeviceB 为上行流量提供的 QoS 限制

Host	CIR(kbit/s)
Host1	2000
Host2	4000
Host3	8000

#### 操作步骤

步骤1 创建VLAN并配置各接口,使Host能够通过DeviceB访问网络。

#在DeviceA上创建VLAN 10、20、30,并将接口加入相应VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 10 20 30
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port default vlan 10
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port default vlan 20
[DeviceA-10GE1/0/2] quit
[DeviceA-10GE1/0/2] quit
[DeviceA] interface 10ge 1/0/3
[DeviceA-10GE1/0/3] portswitch
```

```
[DeviceA-10GE1/0/3] port default vlan 30
[DeviceA-10GE1/0/3] quit
[DeviceA] interface 10ge 1/0/4
[DeviceA-10GE1/0/4] portswitch
[DeviceA-10GE1/0/4] port link-type trunk
[DeviceA-10GE1/0/4] port trunk allow-pass vlan 10 20 30
[DeviceA-10GE1/0/4] quit
```

# 在DeviceB上创建VLAN 10、20、30,并将接口10GE1/0/1加入VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] vlan batch 10 20 30
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] portswitch
[DeviceB-10GE1/0/1] port link-type trunk
[DeviceB-10GE1/0/1] port trunk allow-pass vlan 10 20 30
[DeviceB-10GE1/0/1] quit
```

# 在DeviceB上配置VLANIF接口,并配置IP地址。

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

## 步骤2 配置流分类。

# 在DeviceB上创建流分类c1~c3,对来自不同Host的业务流按照其VLAN ID进行分类。

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

## 步骤3 配置流量监管行为。

#在DeviceB上创建流行为b1~b3,对来自不同Host的报文进行流量监管。

```
[DeviceB] traffic behavior b1
[DeviceB-behavior-b1] car cir 2000
[DeviceB-behavior-b1] statistics enable
[DeviceB-behavior-b1] quit
[DeviceB] traffic behavior b2
[DeviceB-behavior-b2] car cir 4000
[DeviceB-behavior-b2] statistics enable
[DeviceB-behavior-b2] quit
[DeviceB] traffic behavior b3
[DeviceB-behavior-b3] car cir 8000
[DeviceB-behavior-b3] statistics enable
[DeviceB-behavior-b3] quit
```

#### 步骤4 配置流策略并应用到入接口上。

# 在DeviceB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10GE1/0/1入方向上,对来自Host的报文进行流量监管。

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

```
[DeviceB-trafficpolicy-p1] classifier c2 behavior b2
[DeviceB-trafficpolicy-p1] classifier c3 behavior b3
[DeviceB-trafficpolicy-p1] quit
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] traffic-policy p1 inbound
[DeviceB-10GE1/0/1] quit
```

### ----结束

## 检查配置结果

上述配置完成后,在DeviceB上可以查看流量监管的配置信息。

# 查看流分类的配置信息。

```
[DeviceB] display traffic classifier
Traffic Classifier Information:
Classifier: c1
Type: OR
Rule(s):
if-match vlan 10

Classifier: c2
Type: OR
Rule(s):
if-match vlan 20

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

Total classifier number is 3
```

#### # 查看流策略的配置信息。

```
[DeviceB] display traffic policy p1
 Traffic Policy Information:
  Policy: p1
   Classifier: c1
    Type: OR
   Behavior: b1
    Committed Access Rate:
      CIR 2000 (Kbps), PIR 2000 (Kbps), CBS 16000 (Bytes), PBS16000 (Bytes)
      Color Mode: color blind
      Conform Action: pass
      Yellow Action: pass
      Exceed Action: discard
    Statistics: enable
   Classifier: c2
    Type: OR
   Behavior: b2
     Committed Access Rate:
      CIR 4000 (Kbps), PIR 4000 (Kbps), CBS 32000 (Bytes), PBS 32000 (Bytes)
      Color Mode: color blind
      Conform Action: pass
      Yellow Action: pass
      Exceed Action: discard
    Statistics: enable
   Classifier: c3
    Type: OR
   Behavior: b3
     Committed Access Rate:
      CIR 8000 (Kbps), PIR 8000 (Kbps), CBS 64000 (Bytes), PBS 64000 (Bytes)
      Color Mode: color blind
      Conform Action: pass
```

Yellow Action: pass Exceed Action: discard Statistics: enable

#### # 查看10GE1/0/1接口上应用的流策略统计信息。

	[DeviceB] display traffic-policy statistics interface 10ge 1/0/1 inbound Traffic policy: p1, inbound							
Slot: 1 Item	Packets	Bytes	pps	bps				
Matched Passed Dropped Filter CAR	363949175 363949175 0 0 0	465854 465854 0 0 0	6494400 94400 0 0 0	8460795 8460795 0 0	8663854896 8663854896			

可以看出,10GE1/0/1接口上应用的流策略为p1。

## 配置脚本

#### ● DeviceB的配置脚本

```
sysname DeviceB
vlan batch 10 20 30
traffic classifier c1 type or
if-match vlan 10
traffic classifier c2 type or
if-match vlan 20
traffic classifier c3 type or
if-match vlan 30
traffic behavior b1
statistics enable
car cir 2000 kbps
traffic behavior b2
statistics enable
car cir 4000 kbps
traffic behavior b3
statistics enable
car cir 8000 kbps
traffic policy p1
classifier c1 behavior b1 precedence 5
classifier c2 behavior b2 precedence 10
classifier c3 behavior b3 precedence 15
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 10GE1/0/1
portswitch
port link-type trunk
port trunk allow-pass vlan 10 20 30
traffic-policy p1 inbound
```

```
return
DeviceA的配置脚本
sysname DeviceA
vlan batch 10 20 30
interface 10GE1/0/1
portswitch
port default vlan 10
interface 10GE1/0/2
portswitch
port default vlan 20
interface 10GE1/0/3
portswitch
port default vlan 30
interface 10GE1/0/4
portswitch
port link-type trunk
port trunk allow-pass vlan 10 20 30
return
```

## 9.7.5 举例:配置流量监管,对网段的每个 IP 单独限速的示例

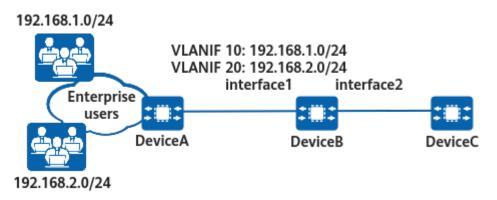
## 组网需求

企业用户通过DeviceA和DeviceB上送报文,经DeviceC与外部网络互通。两个用户使用不同的网段访问网络,现要求对192.168.1.0/24网段**每个IP地址**访问互联网流量限制为64kbit/s,对192.168.2.0/24网段**每个IP地址**访问互联网流量限制为128kbit/s。

#### 图 9-8 配置流量监管的组网图

#### 山 说明

本例中interface1、interface2分别代表10GE1/0/1、10GE1/0/2。



#### 操作步骤

步骤1 创建VLAN并配置各接口,使企业用户能够通过DeviceB访问网络。 # 在DeviceB上创建VLAN 10、20,并将接口10GE1/0/1加入VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] vlan batch 10 20
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] portswitch
[DeviceB-10GE1/0/1] port link-type trunk
[DeviceB-10GE1/0/1] port trunk allow-pass vlan 10 20
[DeviceB-10GE1/0/1] quit
```

#### # 在DeviceB上配置VLANIF接口,并配置IP地址。

```
[DeviceB] interface vlanif 10
[DeviceB-Vlanif10] ip address 192.168.1.1 24
[DeviceB-Vlanif10] quit
[DeviceB] interface vlanif 20
[DeviceB-Vlanif20] ip address 192.168.2.1 24
[DeviceB-Vlanif20] quit
```

#### 步骤2 配置流分类。

# 在DeviceB上创建ACL规则匹配来自企业用户的报文,并创建流分类c1和c2,对来自不同企业用户的业务流按照其IP地址进行分类。

```
[DeviceB] acl 2001
[DeviceB-acl4-basic-2001] rule permit source 192.168.1.0 0.0.0.255
[DeviceB-acl4-basic-2001] quit
[DeviceB] acl 2002
[DeviceB-acl4-basic-2002] rule permit source 192.168.2.0 0.0.0.255
[DeviceB-acl4-basic-2002] quit
[DeviceB] traffic classifier c1
[DeviceB-classifier-c1] if-match acl 2001
[DeviceB-classifier-c1] quit
[DeviceB] traffic classifier c2
[DeviceB-classifier-c2] if-match acl 2002
[DeviceB-classifier-c2] quit
```

#### 步骤3 配置流量监管行为。

# 在DeviceB上创建流行为b1和b2,对来自不同企业用户的报文进行流量监管。

```
[DeviceB] traffic behavior b1
[DeviceB-behavior-b1] car cir 64
[DeviceB-behavior-b1] quit
[DeviceB] traffic behavior b2
[DeviceB-behavior-b2] car cir 128
[DeviceB-behavior-b2] quit
```

#### 步骤4 配置流策略并应用到入接口上。

# 在DeviceB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10GE1/0/1入方向上,对来自两个不同网段的报文进行流量监管。

```
[DeviceB] traffic policy p1
[DeviceB-trafficpolicy-p1] classifier c1 behavior b1
[DeviceB-trafficpolicy-p1] classifier c2 behavior b2
[DeviceB-trafficpolicy-p1] quit
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] traffic-policy p1 inbound
[DeviceB-10GE1/0/1] quit
```

#### ----结束

## 检查配置结果

上述配置完成后,在DeviceB上可以查看流量监管的配置信息。

# 查看流分类的配置信息。

```
[DeviceB] display traffic classifier
 Traffic Classifier Information:
  Classifier: c1
   Type: OR
   Rule(s):
     if-match acl 2001
  Classifier: c2
   Type: OR
   Rule(s):
     if-match acl 2002
```

Total classifier number is 2

#### # 查看流策略的配置信息。

```
[DeviceB] display traffic policy p1
 Traffic Policy Information:
  Policy: p1
   Classifier: c1
    Type: OR
   Behavior: b1
    Committed Access Rate:
      CIR 64 (Kbps), PIR 64 (Kbps), CBS 10000 (Bytes), PBS 10000 (Bytes)
      Color Mode: color blind
      Conform Action: pass
      Yellow Action: pass
      Exceed Action: discard
   Classifier: c2
     Type: OR
   Behavior: b2
     Committed Access Rate:
      CIR 128 (Kbps), PIR 128 (Kbps), CBS 10000 (Bytes), PBS 10000 (Bytes)
      Color Mode: color blind
      Conform Action: pass
      Yellow Action: pass
      Exceed Action: discard
```

### 配置脚本

#### DeviceB的配置脚本

```
sysname DeviceB
vlan batch 10 20
acl 2001
rule permit source 192.168.1.0 0.0.0.255
acl 2002
rule permit source 192.168.2.0 0.0.0.255
traffic classifier c1 type or
if-match acl 2001
traffic classifier c2 type or
if-match acl 2002
traffic behavior b1
car cir 64
traffic behavior b2
car cir 128
traffic policy p1
classifier c1 behavior b1
classifier c2 behavior b2
```

```
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 10GE1/0/1
portswitch
port link-type trunk
port trunk allow-pass vlan 10 20
traffic-policy p1 inbound
#
return
```

# 9.8 配置流量整形

## 背景信息

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

## 9.8.1 配置队列流量整形

## 背景信息

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

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

### 操作步骤

步骤1 进入系统视图。

system-view

步骤2 进入接口视图。

interface { interface-type interface-number | interface-name }

步骤3 配置队列流量整形速率。

qos queue queue-index shaping { percent cir cir-percent-value [ pir pir-percent-value ] | cir cir-value [ kbps | mbps | gbps ] [ cbs cbs-value [ bytes | kbytes | mbytes ] | pir pir-value [ kbps | mbps | gbps ] [ cbs cbs-value [ bytes | kbytes | mbytes ] ] ] }

[ cbs cbs-value [ bytes | kbytes | mbytes ] pbs pbs-value [ bytes | kbytes | mbytes ] ] ] }

缺省情况下,队列的整形速率是接口的最大带宽。

#### □ 说明

仅S6730-H-V2、S5732-H-V2和S5755-H系列支持mbytes参数。

----结束

## 9.8.2 检查配置结果

#### 操作步骤

执行命令display qos configuration interface [{ interface-type interface-number | interface-name }], 查看接口上所有的QoS配置信息。

执行命令display qos queue statistics { slot slotid | interface { interface-type interface-number | interface-name } } , 查看基于队列的流量统计信息。

#### ----结束

## 9.8.3 举例:配置流量整形,对不同业务限速的示例

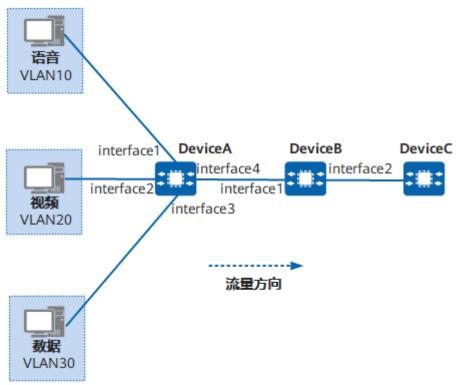
## 组网需求

如图9-9所示,有三台主机分别为用户提供语音、视频、数据业务,通过DeviceA和DeviceB上送报文,经DeviceC与外部网络互通。把连接语音主机的接口划分到VLAN10,把连接视频主机的接口划分到VLAN20,把连接数据主机的接口划分到VLAN30。

#### 图 9-9 流量整形配置组网图

#### □说明

本例中interface1、interface2、interface3、interface4分别代表10GE1/0/1、10GE1/0/2、10GE1/0/3、10GE1/0/4。



语音、视频、数据业务的报文使用802.1p优先级进行标识,分别为5、3、2。当报文从 DeviceB的interface2到达DeviceC时,可能会发生抖动。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:

表 9-12 DeviceB 上为各业务提供的带宽

接口/业务类型	保证带宽(kbit/s)	峰值带宽(kbit/s)
语音	3000	5000

·	妾口/业务类型	保证带宽(kbit/s)	峰值带宽(kbit/s)
礼	见频	5000	8000
*		2000	3000

### 操作步骤

步骤1 在DeviceB上创建VLAN并配置各接口,使用户能够通过DeviceB访问网络。

# 创建VLAN 10、20、30。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] vlan batch 10 20 30
```

# 将接口10GE1/0/1、10GE1/0/2分别以Trunk方式加入VLAN 10、VLAN 20和VLAN 30。

```
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] portswitch
[DeviceB-10GE1/0/1] port link-type trunk
[DeviceB-10GE1/0/1] port trunk allow-pass vlan 10 20 30
[DeviceB-10GE1/0/1] quit
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] portswitch
[DeviceB-10GE1/0/2] port link-type trunk
[DeviceB-10GE1/0/2] port trunk allow-pass vlan 10 20 30
[DeviceB-10GE1/0/2] quit
```

步骤2 配置DeviceA与主机端相连接口的端口优先级,以区分不同业务报文。

#在DeviceA上配置10GE1/0/1、10GE1/0/2、10GE1/0/3的端口优先级为5、3、2,接口10GE1/0/4加入VLAN 10、VLAN 20和VLAN 30。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 10 20 30
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port default vlan 10
[DeviceA-10GE1/0/1] port priority 5
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port default vlan 20
[DeviceA-10GE1/0/2] port priority 3
[DeviceA-10GE1/0/2] quit
[DeviceA] interface 10ge 1/0/3
[DeviceA-10GE1/0/3] portswitch
[DeviceA-10GE1/0/3] port default vlan 30
[DeviceA-10GE1/0/3] port priority 2
[DeviceA-10GE1/0/3] quit
[DeviceA] interface 10ge 1/0/4
[DeviceA-10GE1/0/4] portswitch
[DeviceA-10GE1/0/4] port link-type trunk
[DeviceA-10GE1/0/4] port trunk allow-pass vlan 10 20 30
[DeviceA-10GE1/0/4] quit
```

步骤3 配置端口队列流量整形,限制语音、视频、数据三类业务的带宽。

# 在DeviceB上配置端口队列流量整形,使语音、视频、数据业务的保证带宽分别为 3000kbit/s、5000kbit/s、2000kbit/s。

```
[DeviceB] interface 10ge 1/0/2

[DeviceB-10GE1/0/2] qos queue 5 shaping cir 3000 pir 5000 kpbs

[DeviceB-10GE1/0/2] qos queue 3 shaping cir 5000 pir 8000 kpbs

[DeviceB-10GE1/0/2] qos queue 2 shaping cir 2000 pir 3000 kpbs

[DeviceB-10GE1/0/2] quit
```

### ----结束

## 检查配置结果

#查看10GE1/0/2出方向队列统计计数。

	ue CIR/PIR	<b>qos queue stat</b> Passed (Packets/Bytes	Pass Rate	Dr	opped	Drop Rate (pps/	Drop
0	0 10000000	0	0 0	0	0 0	-	
1	0 10000000	0	0 0	0	0 0	-	
2	2000 3000	54584 5676736	0	0	0	-	
3	5000 8000	49648 5163392	0	0	0	-	
4	0 10000000	0	0	0	0 0	-	
5		49998 5199792		0	0	-	
6	0 10000000	0	0 0	0	0 0	-	
7	0 10000000	0	0	0 0	0 0	-	

### 配置脚本

#### ● DeviceB的配置脚本

```
# sysname DeviceB
# vlan batch 10 20 30
# interface 10GE1/0/1
portswitch
port link-type trunk
port trunk allow-pass vlan 10 20 30
# interface 10GE1/0/2
portswitch
port link-type trunk
port trunk allow-pass vlan 10 20 30
# or trunk allow-pass vlan 10 20 30
qos queue 2 shaping cir 2000 kbps pir 3000 kbps
qos queue 5 shaping cir 5000 kbps pir 8000 kbps
qos queue 5 shaping cir 3000 kbps pir 5000 kbps
# return
```

#### ● DeviceA的配置脚本

```
#
sysname DeviceA
```

```
vlan batch 10 20 30
interface 10GE1/0/1
portswitch
port default vlan 10
port priority 5
interface 10GE1/0/2
portswitch
port default vlan 20
port priority 3
interface 10GE1/0/3
portswitch
port default vlan 30
port priority 2
interface 10GE1/0/4
portswitch
port link-type trunk
port trunk allow-pass vlan 10 20 30
```

# 9.8.4 举例:配置基于 DiffServ 域优先级映射的流量整形

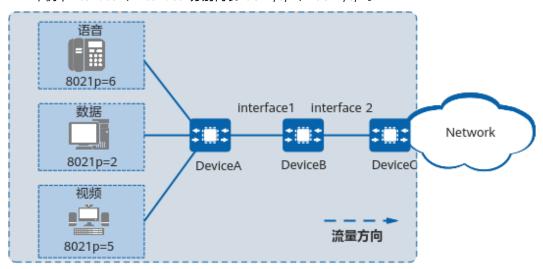
## 组网需求

如<mark>图9-10</mark>所示,来自用户侧的业务有语音、视频、数据,通过DeviceA和DeviceB上送报文,经DeviceC与外部网络互通。

### 图 9-10 流量整形配置组网图

#### 山 说明

本例中interface1、interface2分别代表10GE1/0/1、10GE1/0/2。



语音、视频、数据业务的报文使用802.1p优先级进行标识,分别为6、5、2。接口带宽限制为10000kbit/s。当报文从DeviceB的interface2到达DeviceC时,可能会发生抖动。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:

表 9-13 DeviceB 上为各业务提供的带宽

接口/业务类型	保证带宽(kbit/s)	峰值带宽(kbit/s)
语音	3000	5000
视频	5000	8000
数据	2000	3000

## 操作步骤

步骤1 在DeviceB上创建VLAN并配置各接口,使用户能够通过DeviceB访问网络。

# 创建VLAN 10。

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

# 将接口10GE1/0/1、10GE1/0/2分别以Trunk方式加入VLAN 10。

[DeviceB] **interface 10ge 1/0/1** [DeviceB-10GE1/0/1] **portswitch** 

[DeviceB-10GE1/0/1] port link-type trunk

[DeviceB-10GE1/0/1] port trunk allow-pass vlan 10

[DeviceB-10GE1/0/1] quit

[DeviceB] interface 10ge 1/0/2

[DeviceB-10GE1/0/2] portswitch

[DeviceB-10GE1/0/2] port link-type trunk

[DeviceB-10GE1/0/2] port trunk allow-pass vlan 10

[DeviceB-10GE1/0/2] quit

#### 步骤2 配置优先级映射

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

[DeviceB] diffserv domain ds1

[DeviceB-dsdomain-ds1] **8021p-inbound 6 phb cs7** //将不同业务携带的802.1p优先级映射为不同的PHB行

为,保证其分别进入不同的队列

[DeviceB-dsdomain-ds1] 8021p-inbound 5 phb ef

[DeviceB-dsdomain-ds1] 8021p-inbound 2 phb af2

[DeviceB-dsdomain-ds1] quit

[DeviceB] interface 10ge 1/0/1

[DeviceB-10GE1/0/1] trust upstream ds1

[DeviceB-10GE1/0/1] quit

#### 步骤3 配置接口整形

# 在DeviceB上配置接口整形,将接口速率限制在10000kbit/s。

[DeviceB] interface 10ge 1/0/2

[DeviceB-10GE1/0/2] **qos lr cir 10000 outbound** //在接口的流量出方向配置基于接口的限速,限制总带宽

#### 步骤4 配置端口队列整形

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

[DeviceB-10GE1/0/2] **qos queue 7 shaping cir 3000 pir 5000** //根据PHB与本地优先级缺省的映射关系,配置进入队列7的语音报文带宽为3000kbit/s

[DeviceB-10GE1/0/2] qos queue 5 shaping cir 5000 pir 8000

[DeviceB-10GE1/0/2] qos queue 2 shaping cir 2000 pir 3000 [DeviceB-10GE1/0/2] quit

#### ----结束

## 检查配置结果

#查看10GE1/0/2出方向队列统计计数。

	ue CIR/PIR	<b>qos queue stat</b> Passed (Packets/Bytes	Pass Rate	Dr	opped	Drop Rate (pps/	Drop
0	0 10000000		0 0	0	0 0	-	
1	0 10000000	0	0 0	0	0	-	
2	2000 3000	54584 5676736		0	0	-	
3	0	0	0 0	0	0	-	
4	0	0	0 0	0	0	-	
		49648 5163392		0	0	-	
6	0	0	0 0	0	0 0	-	
7		49998 5199792	0	0	0	-	

## 配置脚本

## ● DeviceB的配置脚本

```
sysname DeviceB
vlan batch 10
diffserv domain ds1
8021p-inbound 6 phb cs7
8021p-inbound 5 phb ef
8021p-inbound 2 phb af2
interface 10GE1/0/1
portswitch
port link-type trunk
port trunk allow-pass vlan 10
trust upstream ds1
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 10
qos lr cir 10000 outbound
qos queue 2 shaping cir 2000 pir 3000
qos queue 5 shaping cir 5000 pir 8000
qos queue 7 shaping cir 3000 pir 5000
return
```

# 9.8.5 举例:配置基于信任 802.1p 优先级的流量整形

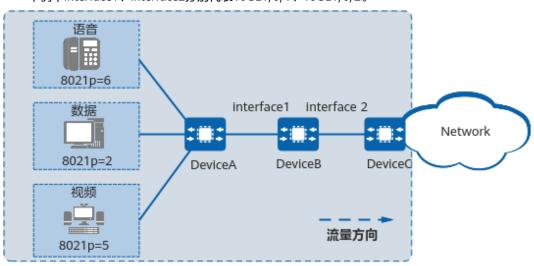
### 组网需求

如<mark>图9-10</mark>所示,来自用户侧的业务有语音、视频、数据,通过DeviceA和DeviceB上送报文,经DeviceC与外部网络互通。

#### 图 9-11 流量整形配置组网图

#### □ 说明

本例中interface1、interface2分别代表10GE1/0/1、10GE1/0/2。



语音、视频、数据业务的报文使用802.1p优先级进行标识,分别为6、5、2。接口带宽限制为10000kbit/s。当报文从DeviceB的interface2到达DeviceC时,可能会发生抖动。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:

表 9-14 DeviceB 上为各业务提供的带宽

接口/业务类型	保证带宽(kbit/s)	峰值带宽(kbit/s)
语音	3000	5000
视频	5000	8000
数据	2000	3000

### 操作步骤

步骤1 在DeviceB上创建VLAN并配置各接口,使用户能够通过DeviceB访问网络。

# 创建VLAN 10。

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

# 将接口10GE1/0/1、10GE1/0/2分别以Trunk方式加入VLAN 10。

[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] portswitch
[DeviceB-10GE1/0/1] port link-type trunk
[DeviceB-10GE1/0/1] port trunk allow-pass vlan 10
[DeviceB-10GE1/0/1] quit
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] portswitch
[DeviceB-10GE1/0/2] port link-type trunk
[DeviceB-10GE1/0/2] port trunk allow-pass vlan 10
[DeviceB-10GE1/0/2] quit

#### 步骤2 配置接口信任报文的类型

#配置接口信任报文的802.1p优先级。

[DeviceB] interface 10ge 1/0/1

[DeviceB-10GE1/0/1] **trust 8021p outer** //配置接口信任802.1p优先级,即报文根据802.1p优先级与本地优先级和队列之间的缺省关系进入不同的队列 [DeviceB-10GE1/0/1] **quit** 

#### 步骤3 配置接口整形

# 在DeviceB上配置接口整形,将接口速率限制在10000kbit/s。

[DeviceB] interface 10ge 1/0/2

[DeviceB-10GE1/0/2] qos lr cir 10000 outbound //在接口的流量出方向配置基于接口的限速,限制总带宽

#### 步骤4 配置端口队列整形

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

[DeviceB-10GE1/0/2] **qos queue 6 shaping cir 3000 pir 5000** //根据PHB与本地优先级缺省的映射关系,配置进入队列7的语音报文带宽为3000kbit/s

[DeviceB-10GE1/0/2] qos queue 5 shaping cir 5000 pir 8000

[DeviceB-10GE1/0/2] qos queue 2 shaping cir 2000 pir 3000

[DeviceB-10GE1/0/2] quit

#### ----结束

## 检查配置结果

# 查看10GE1/0/2出方向队列统计计数。

Que	ue CIR/PIR	qos queue stat Passed (Packets/Bytes	Pass Rat	e Dr	opped	Drop Rate (pps/	Drop
0	0 10000000	0	0	0	0	-	
1	0 10000000	0 0	0 0	0 0	0 0	-	
2	2000 3000	54584 5676736	0 0	0 0	0	-	
3	0 10000000	0 0	0	0 0	0 0	-	
4	0 10000000	0 0	0	0 0	0 0	-	
5	5000 8000	49648 5163392	0	0	0	-	

6 3000 5000	49998 5199792	0	0	0	-
7 0 10000000	0	0	0	0 -	

### 配置脚本

#### DeviceB的配置脚本

```
sysname DeviceB
vlan batch 10
interface 10GE1/0/1
portswitch
port link-type trunk
port trunk allow-pass vlan 10
trust 8021p outer
interface 10GE1/0/1
trust 8021p outer
interface 10GE1/0/2
portswitch
port link-type trunk
port trunk allow-pass vlan 10
qos lr cir 10000 outbound
qos queue 2 shaping cir 2000 pir 3000
qos queue 5 shaping cir 5000 pir 8000
qos queue 6 shaping cir 3000 pir 5000
1/0/1
return
```

## 9.9 配置接口限速

## 背景信息

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

## 9.9.1 配置流量监管实现接口限速

## 背景信息

如果不限制用户发送的流量,大量用户不断突发的数据会使网络更拥挤。可以在当前 网络设备的入接口上配置流量监管功能,将通过某个接口进入网络的流量限制在一个 合理的范围内,当收到报文的速率大于流量监管速率时,主动将超出部分的报文丢弃。

## 操作步骤

**步骤1** 进入系统视图。 system-view

步骤2 (可选)配置计算流量监管的速率时不包括报文的帧间隙和前导码。

qos car ifg disable

#### 步骤3 创建并配置CAR模板。

qos car car-name { percent percent-value | cir cir-value [ kbps | mbps | gbps ] [ cbs cbs-value [ bytes | kbytes | mbytes ] [ pbs pbs-value [ bytes | kbytes | mbytes ] ] | pir pir-value [ kbps | mbps | gbps ] [ cbs cbs-value [ bytes | kbytes | mbytes ] pbs pbs-value [ bytes | kbytes | mbytes ] ] ] }

CAR模板中定义的是流量监管的限速速率。

#### 步骤4 进入接口视图。

interface { interface-type interface-number | interface-name }

#### 步骤5 在接口入方向上应用CAR模板。

qos car inbound car-name

接口入方向上应用CAR模板后,设备对流入该接口的所有业务流量实施限速。

----结束

### 检查配置结果

- 执行命令display qos car [ car-name ],查看CAR模板的配置信息。
- 执行命令display qos car statistics interface { interface-type interface-number | interface-name } inbound, 查看配置流量监管实现接口限速后,指定接口上通过和丢弃的报文统计信息。

## 9.9.2 配置流量整形实现接口限速

## 背景信息

为了防止下游网络向相邻的上游网络发送数据流量过大,造成拥塞或大量报文的直接丢弃,可以在当前网络设备的出接口上配置流量整形功能,限制流出某一连接的流量与突发,使报文均匀地向外发送。配置流量整形实现接口限速后,当报文的发送速率超过限制速率时,超出的那部分报文先进入缓存队列;当令牌桶有足够的令牌时,再均匀向外发送这些被缓存的报文;当缓存队列已满时,新到达的报文将被丢弃。

如果报文经过VPN隧道封装,当设备在WAN侧接口上做QoS限速或者流量统计时,实际计算的报文长度包含链路层和物理层报文头长度以及各种隧道协议封装头长度,这种方式计算出来的用户实际带宽会比预期值小。为了减小用户实际带宽与预期值之间的差距,可以配置报文长度的计算方式为不包括报文的帧间隙和前导码,以及配置减去Tunnel接口下报文隧道封装长度功能,这样计算的报文长度会减去物理层报文头长度和隧道协议封装头的长度。

#### □ 说明

通过流量整形实现接口限速,当前只支持对接口的出方向进行限速。 当接口出方向的流量速率大于配置的出方向的接口限速的告警阈值时会产生告警。

#### 操作步骤

步骤1 进入系统视图。

system-view

步骤2 进入接口视图。

interface { interface-type interface-number | interface-name }

#### 步骤3 配置接口出方向的限速速率。

qos lr cir cir-value [ kbps | mbps | gbps ] [ cbs cbs-value [ bytes | kbytes | mbytes ] ] [ outbound ]

缺省情况下,接口限速速率为接口的最大带宽。

#### □说明

仅S6730-H-V2、S5732-H-V2和S5755-H系列支持mbytes参数。

#### ----结束

## 9.9.3 配置管理网口的流量限速

## 背景信息

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

#### □ 说明

仅S6730-H-V2、S5732-H-V2和S5755-H系列支持该功能。

### 操作步骤

#### 步骤1 进入系统视图。

system-view

#### 步骤2 进入管理网口视图。

interface meth 0/0/0

#### 步骤3 配置管理网口的流量限速。

qos lr pps packets

#### □ 说明

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

#### ----结束

### 检查配置结果

- 在管理网口视图执行命令display this interface,通过显示信息中的Over-carpps字段可以查看超出管理网口限速值而丢失的流量。
- 在任意视图执行命令display interface meth 0/0/0,通过显示信息中的Overcar-pps字段可以查看超出管理网口限速值而丢失的流量。

## 9.9.4 举例: 配置流量监管实现接口限速

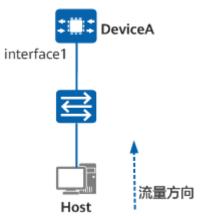
#### 组网需求

如<mark>图9-12</mark>所示,Host通过DeviceA上送报文,要求Host上送报文的带宽不超过100Mbit/s。

#### 图 9-12 接口限速配置组网图

#### □ 说明

本例中interface1代表10GE1/0/1。



## 操作步骤

#### 步骤1 配置CAR模板。

# 在DeviceA上创建CAR模板car1,对Host的流量进行监管。

<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] qos car car1 cir 100000

#### 步骤2 应用CAR模板。

#在DeviceA的接口10GE1/0/1的入方向应用模板car1,对Host的流量进行监管。

[DeviceA] interface 10ge 1/0/1 [DeviceA-10GE1/0/1] qos car inbound car1 [DeviceA-10GE1/0/1] quit

#### ----结束

## 检查配置结果

# 查看CAR模板的配置信息。

# 分别使用60000kbit/s和110000kbit/s的速率向接口10GE1/0/1输入报文流,然后使用命令**display qos car statistics**查看流量统计信息。如果配置成功:使用60000kbit/s向接口10GE1/0/1输入报文流时,报文全部转发,无丢弃报文;使用110000kbit/s向接口10GE1/0/1输入报文流时,报文有部分丢弃。

## 配置脚本

#### DeviceA的配置脚本

```
#
sysname DeviceA
#
qos car car1 cir 100000 kbps
#
interface 10GE1/0/1
qos car inbound car1
#
return
```

# 9.10 配置 QoS 模板

## 背景信息

QoS模板视图下可以配置流量监管、报文处理优先级,目前仅在AAA的业务方案下绑定QoS模板,用于用户授权。

### 操作步骤

步骤1 进入系统视图

system-view

步骤2 创建QoS模板并进入QoS模板视图。

qos-profile profile-name

步骤3 在QoS模板视图下配置流量监管、报文处理优先级。

- 配置流量监控。
  - car cir cir-value [ pir pir-value ] [ cbs cbs-value pbs pbs-value ] { inbound | outbound }
- 重标记IP报文的DSCP优先级。
   remark dscp dscp-value { inbound | outbound }
- 重标记VLAN报文的802.1p优先级。 remark 8021p 8021p-value { inbound | outbound

#### ----结束

## 检查配置结果

- 执行命令display qos-profile profile-name, 查看指定QoS模板的配置信息。
- 执行命令display qos-profile all, 查看所有QoS模板的配置信息。

## 9.11 维护流量监管、流量整形和接口限速

## 背景信息

#### 须知

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

## 操作步骤

- 配置流量监管实现接口限速后,清除指定接口上通过和丢弃的报文统计信息。 reset qos car statistics interface { interface-type interface-number | interface-name } inbound
- 清除基于队列的流量统计信息 reset qos queue statistics { interface { interface-type interface-number | interface-name } | slot slot-id }

----结束

## 10 拥塞避免配置

- 10.1 拥塞避免简介
- 10.2 拥塞避免原理描述
- 10.3 拥塞避免配置注意事项
- 10.4 拥塞避免缺省配置
- 10.5 配置WRED
- 10.6 配置CFI作为内部丢弃优先级
- 10.7 检查配置结果
- 10.8 维护拥塞避免
- 10.9 举例: 配置WRED

## 10.1 拥塞避免简介

#### 定义

拥塞避免是指通过监控网络资源(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拥塞控制机 制。

#### 目的

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。然而在多种业务并存的复杂环境下,网络拥塞又极为常见。拥塞避免就 是通过一定的丢弃算法来避免拥塞加剧,同时又可充分利用网络带宽。

## 10.2 拥塞避免原理描述

### 10.2.1 WRED 原理

拥塞避免常用的两种丢弃报文方式为尾丢弃(Tail Drop)和WRED(Weighted Random Early Detection) 。

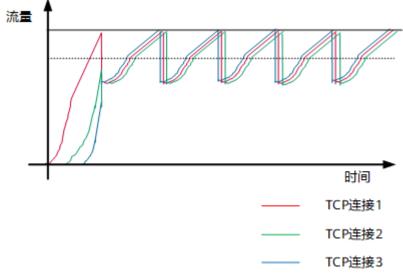
#### 尾丟弃

传统的丢包策略采用尾部丢弃的方法。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。

这种丟弃策略会引发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。

流量

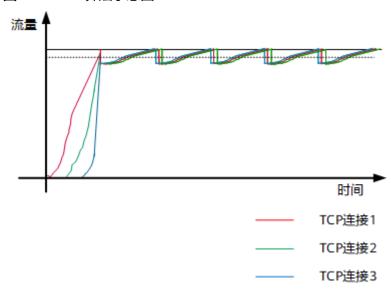
图 10-1 尾部丢包示意图



#### **WRED**

为避免TCP全局同步现象,出现了RED(Random Early Detection)技术。RED通过随 机地丟弃数据报文,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。

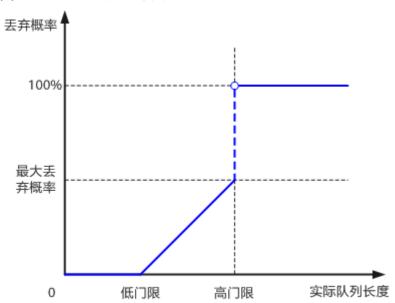




基于RED技术,设备实现了WRED。接口或者接口队列上应用丢弃模板后,报文根据丢弃模板被丢弃。丢弃模板设置报文丢包的上下门限及丢包率,报文到达下限时,开始丢包,随着门限的增高,丢包率不断增加,最高丢包率不超过设置的丢包率,直至到达高门限,报文全部丢弃,这样按照一定的丢弃概率主动丢弃队列中的报文,从而一定的程度上避免拥塞问题。

WRED丢弃概率曲线如图10-3所示。

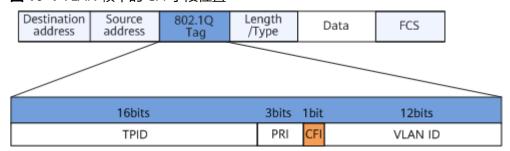
图 10-3 WRED 丟弃概率曲线



## 10.2.2 用 CFI 作为内部丢弃优先级原理

通常二层设备之间交互VLAN帧。根据IEEE 802.1Q定义,VLAN帧头中的CFI(Canonical Format Indicator)又称为DEI(Drop Eligible Indicator),可以用来标识报文的丢弃优先级。VLAN帧中的CFI字段位置如<mark>图10-4</mark>所示。

图 10-4 VLAN 帧中的 CFI 字段位置



VLAN标记中的CFI字段,取值范围是0或1。设备在配置CFI作为内部丢弃优先级后,对超出承诺信息速率CIR的报文的DEI位设置为1,标识该报文的丢弃优先级为高,后续设备在拥塞时优先丢弃DEI位为1的报文。

## 10.3 拥塞避免配置注意事项

#### License 依赖

拥塞避免无需License许可即可使用。

## 硬件依赖

表 10-1 支持本特性的硬件

系列	支持产品
S5735-L-V2 series	S5735-L10T4X-A-V2/S5735-L14P2S-QA-V2/S5735-L16LP2UM2X-QA-V2/S5735-L16LP2X-QA-V2/S5735-L16P2UM2X-QA-V2/S5735-L16T4S-A-V2/S5735-L16T4X-QA-V2/S5735-L24P4S-A-V2/S5735-L24P4XE-A-V2/S5735-L24P4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L24T4XE-A-V2/S5735-L48LP4S-A-V2/S5735-L48LP4XE-A-V2/S5735-L48P4XE-A-V2/S5735-L48S4XE-A-V2/S5735-L48S4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L48T4XE-A-V2/S5735-L8P4X-A-V2/S5735-L
S5735-S-V2 series	S5735-S24HS4XE-V2/S5735-S24P4XE-V2/S5735- S24ST4XE-V2/S5735-S24T4XE-V2/S5735- S24U4XE-V2/S5735-S48HS4XE-V2/S5735- S48P4XE-V2/S5735-S48S4XE-V2/S5735-S48T4XE- V2/S5735-S48U4XE-V2
S5735I-L-V2 series	S5735I-L10T4X-A-V2/S5735I-L8P4X-A-V2

系列	支持产品
S5755-H series	S5755-H24N4Y-A/S5755-H24P4Y2CZ/S5755- H24T4Y2CZ/S5755-H24U4Y2CZ/S5755- H24UN4Y2CZ/S5755-H24UTM4X4Y2C/S5755- H48N4Y-A/S5755-H48P4Y2CZ/S5755-H48T4Y2CZ/ S5755-H48U4Y2CZ/S5755-H48UN4Y2CZ/S5755- H48UTM4X4Y2C
S6730-H-V2 series	S6730-H24X6C-V2/S6730-H28X6CZ-V2/S6730- H48X6C-V2/S6730-H48X6CZ-V2/S6730-H48Y6C- V2
S5732-H-V2 series	S5732-H24S4X6QZ-V2/S5732-H24UM4Y2CZ-KV2/ S5732-H24UM4Y2CZ-V2/S5732-H44S4X6QZ-V2/ S5732-H48UM4Y2CZ-KV2/S5732-H48UM4Y2CZ- V2
S5735I-H-V2 series	S5735I-H8T4S2XN-V2
S5735I-S-V2 series	S5735I-S24T4XE-V2/S5735I-S24U4XE-V2/S5735I- S8T4SN-V2/S5735I-S8T4XN-V2/S5735I-S8U4XN- V2

### 特性限制

表 10-2 本特性的使用限制

特性限制	系列	涉及产品
在多个端口往一个端口发送流量时,如果流量存在突发且突发数据量超过分配的缓存最大值,则设备会对超过的报文进行丢包。因此,对于流量突发比较多且需要多个端口同时往一个端口发送流量的场景,请通过qos burst-mode 命令设置缓存管理的突发模式为非标准模式,以提高设备对突发流量的转发能力。	S5735-S-V2 series S5735-L-V2 series S5735I-L-V2 series S5755-H series S6730-H-V2 series S5732-H-V2 series S5735I-S-V2 series S5735I-H-V2 series	S5735-S24HS4XE-V2/S5735-S24P4XE-V2/S5735-S24ST4XE-V2/S5735-S24T4XE-V2/S5735-S24U4XE-V2/S5735-S48HS4XE-V2/S5735-S48HS4XE-V2/S5735-S48U4XE-A-V2/S5735-S48U4XE-A-V2/S5735-S48U4XE-A-V2/S5735-S48U4XE-A-V2/S5735-S48U4XE-A-V2/S5735-S48U4XE-A-V2/S5735-S48U4XE-A-V2/S5735-S48U4XE-A-V2/S5735-S48U4XE-A-V2/S5735-S5

特性限制	系列	涉及产品
		L48T4XE-A-V2/ S5735-L48T4XE- D-V2/S5735- L8P2T4X-A-V2/ S5735-L8P4S-A- V2/S5735-L8P4X- QA-V2/S5735- L8T4S-A-V2/ S5735-L8T4X-QA- V2
		S5735I-L10T4X-A- V2/S5735I-L8P4X- A-V2
		S5755-H24N4Y-A/ S5755- H24P4Y2CZ/ S5755- H24T4Y2CZ/ S5755- H24U4Y2CZ/ S5755- H24UN4Y2CZ/ S5755- H24UTM4X4Y2C/ S5755-H48N4Y-A/ S5755- H48T4Y2CZ/ S5755- H48UY2CZ/ S5755- H48UY2CZ/ S5755- H48UY2CZ/ S5755- H48UN4Y2CZ/
		S6730-H24X6C- V2/S6730- H28X6CZ-V2/ S6730-H48X6C- V2/S6730- H48X6CZ-V2/ S6730-H48Y6C-V2
		S5732- H24S4X6QZ-V2/ S5732- H24UM4Y2CZ- KV2/S5732- H24UM4Y2CZ-V2/ S5732-

特性限制	系列	涉及产品
		H44S4X6QZ-V2/ S5732- H48UM4Y2CZ- KV2/S5732- H48UM4Y2CZ-V2
		S5735I-S24T4XE- V2/S5735I- S24U4XE-V2/ S5735I-S8T4SN- V2/S5735I- S8T4XN-V2/ S5735I-S8U4XN- V2
		S5735I- H8T4S2XN-V2

## 10.4 拥塞避免缺省配置

表 10-3 拥塞避免缺省配置

参数	缺省配置
WRED丟弃功能	未启用
WRED丢弃的下限百分比	100
WRED丢弃的上限百分比	100
WRED的最大丟弃概率	100
WRED的丢弃门限绝对值	未配置

## 10.5 配置 WRED

## 背景信息

WRED技术基于丢弃参数随机丢弃报文,以避免TCP全局同步现象。它通过报文的不同颜色(丢弃优先级)来指定不同的丢弃策略,考虑了高优先级报文的利益并使其被丢弃的概率相对较小。通过配置WRED丢弃模板可以配置不同颜色(丢弃优先级)报文的丢弃门限绝对值、丢弃门限百分比和最大丢弃概率。

丢弃优先级用在拥塞避免时识别是否丢包,对内部优先级与队列的映射关系没有影响。

#### 操作步骤

步骤1 进入系统视图。

system-view

步骤2 创建WRED丢弃模板,并进入WRED丢弃模板视图。

drop-profile drop-profile-name

缺省情况下,设备中存在一个名为default的WRED丢弃模板。

对于S6730-H-V2、S5732-H-V2和S5755-H系列,设备最多支持配置63个WRED丢弃模板,其中包括default丢弃模板。default丢弃模板不能删除,只能修改参数。

对于S5735I-S-V2、S5735-L-V2、S5735-S-V2、S5735I-L-V2、S5735I-H-V2系列,设备最多支持配置30个WRED丢弃模板,其中包括default丢弃模板。default丢弃模板不能删除,只能修改参数。

#### 步骤3 配置WRED参数。

color { green | red | yellow } { buffer-size low-limit low-buffer-size high-limit high-buffer-size | buffer-size cell low-limit low-buffer-size-cell high-limit high-buffer-size-cell | low-limit low-limit-percentage high-limit high-limit-percentage discard-percentage

缺省情况下,WRED丢弃模板的丢弃上下门限百分比和最大丢弃概率值均为100,未配置丢弃门限绝对值。

#### □ 说明

仅S6730-H-V2、S5732-H-V2和S5755-H系列支持配置**buffer-size**参数,即丢弃门限绝对值。

步骤4 退出WRED丢弃模板视图。

quit

步骤5 进入接口视图。

interface { interface-type interface-number | interface-name }

步骤6 将WRED丢弃模板应用于端口队列。

qos queue queue-index wred drop-profile-name

步骤7 退出接口视图。

quit

----结束

## 10.6 配置 CFI 作为内部丢弃优先级

#### 背景信息

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

如果用户希望在后续处理时丢弃之前超出CIR的报文,可以使用该配置。

#### 操作步骤

步骤1 进入系统视图。

system-view

步骤2 进入接口视图。

interface { interface-type interface-number | interface-name }

步骤3 配置CFI作为内部丢弃优先级。

dei enable

步骤4 退出接口视图。

quit

----结束

## 10.7 检查配置结果

#### 操作步骤

- 执行命令display drop-profile [ drop-profile-name | brief ], 查看WRED丟弃模板的配置信息。
- 执行命令**display qos configuration interface** [ { *interface-type interface-number* | *interface-name* } ],查看接口上所有的QoS配置信息。
- 执行命令display qos queue statistics { slot slotid | interface { interface-type interface-number | interface-name } } , 查看基于队列的流量统计信息。

----结束

## 10.8 维护拥塞避免

#### 背景信息

#### 须知

清除统计信息后,以前的统计信息将无法恢复,务必仔细确认。

#### 操作步骤

● 清除基于队列的流量统计信息。

reset qos queue statistics { interface { interface-type interface-number | interface-name } | slot slot-id }

----结束

## 10.9 举例: 配置 WRED

#### 组网需求

来自Host1和Host2的业务有语音、视频、数据,这些业务可经由DeviceB和DeviceA到达用户,为了减轻网络拥塞造成的影响,保证用户对于高优先级、低延迟业务的服务要求,配置需求如表10-4所述。

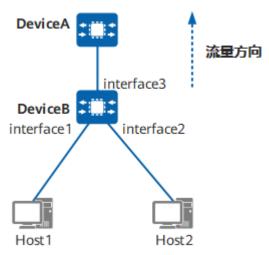
<b>从 10-4</b> 洲本姓尤癿自令奴	表	10-4	拥塞避免配置参数
------------------------	---	------	----------

业务类型	设备丢弃优 先级	阈值下限 (%)	阈值上限 (%)	丢弃概率 (%)	设备内部优 先级
语音	绿	80	100	10	EF
视频	黄	60	80	20	AF3
数据	红	40	60	40	AF1

#### 图 10-5 拥塞避免组网图

#### □ 说明

本例中interface1、interface2和interface3分别代表10GE1/0/1, 10GE1/0/2和10GE1/0/3。



#### 操作步骤

步骤1 配置各接口所属的VLAN,使各设备间链路互通。

# 配置DeviceB接口10GE1/0/3的接口类型为trunk,并将接口10GE1/0/1加入 VLAN100,接口10GE1/0/2加入VLAN200,接口10GE1/0/3加入VLAN100和 VLAN200。

<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] vlan batch 100 200
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] port default vlan 100
[DeviceB-10GE1/0/1] quit
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] port default vlan 200
[DeviceB-10GE1/0/2] quit
[DeviceB] interface 10ge 1/0/3
[DeviceB-10GE1/0/3] port link-type trunk
[DeviceB-10GE1/0/3] port trunk allow-pass vlan 100 200
[DeviceB-10GE1/0/3] quit

**步骤2** 配置优先级映射,根据802.1p值将语音、数据、视频映射为不同的设备内部优先级和 丢弃优先级,实现对报文的分类。 # 创建DiffServ域ds1,将802.1p值6、5、2分别映射为设备内部优先级EF、AF3、AF1,并分别将设备丢弃优先级标记为绿色、黄色、红色。

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

# 在DeviceB入接口10GE1/0/1和10GE1/0/2上绑定DiffServ域。

```
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] trust upstream ds1
[DeviceB-10GE1/0/1] quit
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] trust upstream ds1
[DeviceB-10GE1/0/2] quit
```

步骤3 配置拥塞避免,通过配置WRED丢弃模板,实现在拥塞发生时,对拥塞的缓解和解除。

# 在DeviceB上创建WRED丢弃模板wred1,并配置wred1的三色报文参数。

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

# 在DeviceB出接口队列上应用WRED丢弃模板wred1。

```
[DeviceB] interface 10ge 1/0/3

[DeviceB-10GE1/0/3] qos queue 5 wred wred1

[DeviceB-10GE1/0/3] qos queue 3 wred wred1

[DeviceB-10GE1/0/3] qos queue 1 wred wred1

[DeviceB-10GE1/0/3] quit
```

#### ----结束

#### 检查配置结果

# 查看DiffServ域ds1的配置信息,可以看到DiffServ域中将802.1p值6、5、2分别映射为设备内部优先级EF、AF3、AF1,并分别将设备丢弃优先级标记为绿色、黄色、红色。

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

# 查看WRED丢弃模板配置信息,可以看到wred1的三色报文参数。

```
Yellow Percentage 60 80 % 20
Red Percentage 40 60 % 40
```

# 查看接口10GE1/0/3的配置信息,可以看到各服务等级队列的调度参数。

```
<DeviceB> display qos configuration interface 10GE 1/0/3
interface 10GE1/0/3
trust flag
            : outer 8021p
diffserv domain : default
             : disable
dei enable
port priority
              : 0
phb marking 8021p : enable
phb marking dscp : disable
phb marking exp : -
port wred
port lr
             : cir = -, cbs = -
port car inbound : -
port car outbound: -
schedule profile : -
            shaping
queue
                        schedule wred
        cir
              pir
        cbs
               pbs
0
                   pq
                    pq
                            wred1
2
                    pq
3
                            wred1
                    pq
                    pq
5
                             wred1
                    pq
6
                    pq
                    pq
```

#### 配置脚本

#### DeviceB的配置脚本。

```
#
sysname DeviceB
#
drop-profile wred1
color green low-limit 80 high-limit 100 discard-percentage 10
color yellow low-limit 60 high-limit 80 discard-percentage 20
color red low-limit 40 high-limit 60 discard-percentage 40
#
vlan batch 100 200
#
diffserv domain ds1
8021p-inbound 2 phb af1 red
8021p-inbound 5 phb af3 yellow
8021p-inbound 6 phb ef green
```

```
#
interface 10GE1/0/1
port default vlan 100
trust upstream ds1
#
interface 10GE1/0/2
port default vlan 200
trust upstream ds1
#
interface 10GE1/0/3
port link-type trunk
port trunk allow-pass vlan 100 200
qos queue 1 wred wred1
qos queue 5 wred wred1
#
return
```

## **1** 用塞管理配置

- 11.1 拥塞管理简介
- 11.2 拥塞管理原理描述
- 11.3 拥塞管理配置注意事项
- 11.4 拥塞管理缺省配置
- 11.5 配置拥塞管理
- 11.6 (可选)配置缓存管理
- 11.7 维护拥塞管理
- 11.8 举例:配置拥塞管理
- 11.9 举例: 配置拥塞避免和拥塞管理综合示例 (PQ+WDRR调度和WRED模板)
- 11.10 微突发检测

## 11.1 拥塞管理简介

#### 定义

拥塞管理就是在网络间歇性出现拥塞,时延敏感业务要求得到比其他业务更高质量的 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服务的一种拥塞控制 机制。

#### 目的

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。然而在多种业务并存的复杂环境下,网络拥塞又极为常见。当网络发生 拥塞时,报文会在队列中缓存,此时拥塞管理会提供某种调度算法安排报文的转发次序,保障一些需要更高质量的QoS服务的业务比如时延敏感业务可以优先调度。

## 11.2 拥塞管理原理描述

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。

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

#### 常见的队列调度技术

■ PQ(SP)调度

绝对优先级PQ(Priority Queuing)调度,又称为SP(Strict Priority)调度。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,将关键业务的报文放入较高优先级的队列,将非关键业务(如E-Mail)的报文放入较低优先级的队列,可以保证关键业务的报文被优先传送,非关键业务的报文在处理关键业务数据的空闲间隙被传送。

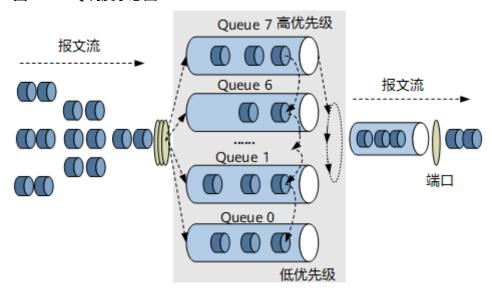
如**图11-1**所示,Queue7比Queue6具有更高的优先权,Queue6比Queue5具有更高的优先权,依次类推。当链路传输报文时,Queue7将优先被服务。只有当Queue7为空,调度器才考虑Queue6。当Queue6有报文等待传输且Queue7为空时,Queue6以链路速率接收类似地服务。当Queue7和Queue6为空时,Queue5以链路速率接收服务,以此类推。

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的报文到达时,则报文将得到优先服务。

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 11-1 PQ 调度示意图



#### WDRR调度

加权差分轮询WDRR(Weighted Deficit Round Robin)调度,在调度过程中考虑包长的因素以达到调度的速率公平性。

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

#### 图 11-2 队列权重示意图

800

如**图11-2**所示,假设用户配置各队列权重为40、30、20、10、40、30、20、10 (依次对应Q7、Q6、Q5、Q4、Q3、Q2、Q1、Q0),调度时,队列Q7、Q6、 Q5、Q4、Q3、Q2、Q1、Q0依次能够获取20%、15%、10%、5%、20%、 15%、10%、5%的带宽。下面以Q7、Q6为例,简要描述WDRR队列调度的实现 过程(假设Q7队列获取400byte/s的带宽,Q6队列获取300byte/s的带宽)。

600

#### - 第1轮调度

700

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。

WDRR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,带宽资源分配不均的缺点。 但是,WDRR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。

#### 不同调度模式间的调度顺序

所有的8个端口队列可以全部配置成某一种调度模式,也可以不同调度模式间组合使用,其中PQ+WDRR调度是业界最常用的一种组合模式。

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

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

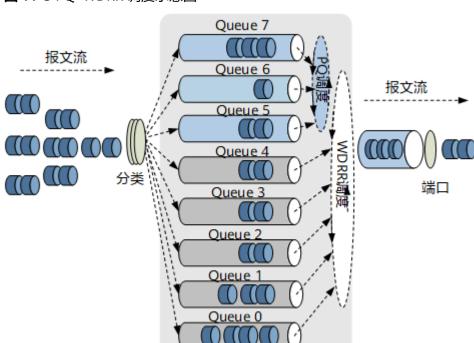


图 11-3 PQ+WDRR 调度示意图

如<mark>图11-3</mark>所示,在调度时,设备首先按照PQ方式优先调度Queue7、Queue6和Queue5队列中的报文流,只有这些队列中的报文流全部调度完毕后,才开始以WDRR方式调度Queue4、Queue3、Queue2、Queue1和Queue0队列中的报文流。其中,Queue4、Queue3、Queue2、Queue1和Queue0队列包含自己的权值。

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

## 11.3 拥塞管理配置注意事项

#### License 依赖

拥塞管理无需License许可即可使用。

### 硬件依赖

表 11-1 支持本特性的硬件

系列	支持产品
S5735-L-V2 series	\$5735-L10T4X-A-V2/\$5735-L14P2S-QA-V2/\$5735-L16LP2UM2X-QA-V2/\$5735-L16LP2X-QA-V2/\$5735-L16P2UM2X-QA-V2/\$5735-L16T4S-A-V2/\$5735-L16T4X-QA-V2/\$5735-L24P4S-A-V2/\$5735-L24P4XE-A-V2/\$5735-L24ST4XE-A-V2/\$5735-L24T4S-A-V2/\$5735-L24T4XE-D-V2/\$5735-L24T4XE-A-V2/\$5735-L24T4XE-A-V2/\$5735-L48LP4S-A-V2/\$5735-L48LP4XE-A-V2/\$5735-L48P4XE-A-V2/\$5735-L48S4XE-A-V2/\$5735-L48S4XE-A-V2/\$5735-L48T4S-A-V2/\$5735-L48T4XE-A-V2/\$5735-L48T4XE-A-V2/\$5735-L48T4XE-A-V2/\$5735-L48T4XE-A-V2/\$5735-L48T4XE-A-V2/\$5735-L8P4X-QA-V2/\$5735-L8P4X-QA-V2/\$5735-L8P4X-QA-V2/\$5735-L8P4X-QA-V2/\$5735-L8T4X-QA-V2
S5735-S-V2 series	S5735-S24HS4XE-V2/S5735-S24P4XE-V2/S5735- S24ST4XE-V2/S5735-S24T4XE-V2/S5735- S24U4XE-V2/S5735-S48HS4XE-V2/S5735- S48P4XE-V2/S5735-S48S4XE-V2/S5735-S48T4XE- V2/S5735-S48U4XE-V2
S5735I-L-V2 series	S5735I-L10T4X-A-V2/S5735I-L8P4X-A-V2
S5755-H series	S5755-H24N4Y-A/S5755-H24P4Y2CZ/S5755- H24T4Y2CZ/S5755-H24U4Y2CZ/S5755- H24UN4Y2CZ/S5755-H24UTM4X4Y2C/S5755- H48N4Y-A/S5755-H48P4Y2CZ/S5755-H48T4Y2CZ/ S5755-H48U4Y2CZ/S5755-H48UN4Y2CZ/S5755- H48UTM4X4Y2C
S6730-H-V2 series	S6730-H24X6C-V2/S6730-H28X6CZ-V2/S6730- H48X6C-V2/S6730-H48X6CZ-V2/S6730-H48Y6C- V2
S5732-H-V2 series	S5732-H24S4X6QZ-V2/S5732-H24UM4Y2CZ-KV2/ S5732-H24UM4Y2CZ-V2/S5732-H44S4X6QZ-V2/ S5732-H48UM4Y2CZ-KV2/S5732-H48UM4Y2CZ- V2
S5735I-H-V2 series	S5735I-H8T4S2XN-V2
S5735I-S-V2 series	S5735I-S24T4XE-V2/S5735I-S24U4XE-V2/S5735I- S8T4SN-V2/S5735I-S8T4XN-V2/S5735I-S8U4XN- V2

## 特性限制

无

## 11.4 拥塞管理缺省配置

表 11-2 拥塞管理缺省配置

参数	缺省配置
拥塞管理功能	已启用
端口队列的调度方式	PQ调度
WDRR调度模式的队列权值	1
缓存管理的突发模式	标准模式
手工配置缓存空间的大小	未配置

## 11.5 配置拥塞管理

#### 背景信息

拥塞管理是一项基于队列的技术。当网络发生拥塞时,报文会在队列中缓存,此时可以配置拥塞管理,设备将按照指定的调度策略决定报文转发时的处理次序,以达到高 优先级报文优先被调度的目的。

设备上每个接口有8个端口队列,不同的队列可以采用不同的队列调度模式。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,队列索引越大,优先级越高。PQ队列调度完成后,再对WDRR队列进行加权轮询调度。

#### 操作步骤

- 对于S6730-H-V2、S5732-H-V2和S5755-H系列:
  - a. 进入系统视图。

system-view

b. 进入接口视图。

interface { interface-type interface-number | interface-name }

c. 配置端口队列的调度方式。

qos { pq { start-queue-index [ to end-queue-index ] } &<1-8> | drr { start-queue-index [ to end-queue-index ] } &<1-8> }\*

缺省情况下,端口队列的调度模式为PQ调度模式。

(可选)配置WDRR调度模式的队列权值。

qos queue queue-index drr weight weight-value

缺省情况下,WDRR调度模式的队列权值为1。

- 对于S5735I-S-V2、S5735-L-V2、S5735I-L-V2、S5735-S-V2、S5735I-H-V2系列:
  - a. 进入系统视图。

system-view

b. 创建全局调度模板,并进入调度模板视图。

qos schedule-profile profile-name

缺省情况下,设备预定义了一个名为default的全局调度模板。

#### □ 说明

除default全局调度模板外,设备最多允许创建11个全局调度模板。对于default全局调度模板,用户只能修改其队列调度模式和队列调度权重,不能删除。

c. 配置端口队列的调度模式。

**qos** { pq { start-queue-index [ to end-queue-index ] } &<1-8> | drr { start-queue-index [ to end-queue-index ] } &<1-8> }\*

缺省情况下,端口队列的调度模式为PQ调度模式。

d. (可选)配置WDRR调度模式的队列权值。

qos queue queue-index drr weight weight-value

缺省情况下,WDRR调度模式的队列权值为1。

e. 退出调度模板视图。

auit

f. 进入接口视图。

interface { interface-type interface-number | interface-name }

q. 应用调度模板。

qos schedule-profile profile-name

缺省情况下,端口下应用调度模板的是default模板。

#### ----结束

#### 检查配置结果

执行命令**display qos queue statistics** { **slot** *slotid* | **interface** { *interface-type interface-number* | *interface-name* } } , 查看基于队列的流量统计信息。

## 11.6 (可选)配置缓存管理

## 11.6.1 了解缓存管理

设备中数据缓冲区(又称为缓存空间)可以用来缓存报文,防止出现由于突发流量导致拥塞而产生的丢包现象。当设备的缓冲区资源被耗尽时,端口队列将不能再缓存报文,未进入缓冲区的报文将直接被丢弃,因此单纯通过队列调度无法在存在较大突发流量的时候保障高优先级业务的转发。缓存管理支持对缓存空间进行合理分配,调整设备的缓存能力,提高设备性能。

芯片上的所有端口共用芯片的缓存空间,端口上的所有队列共用该端口的缓存空间。 缓存空间可以划分为芯片级、端口级、队列级。

## 11.6.2 配置缓存管理的突发模式

#### 背景信息

设备中的缓存空间采用"静态+动态"的方式进行分配。每个端口默认分配一部分静态缓存,用于保证队列的最基本转发能力;剩余缓存作为动态缓存,用于保证队列的突

发转发能力,当队列中存在突发报文时,可以使用动态缓存,设备支持的缓存模式如表11-3所示。

在多个端口往一个端口发送流量时,如果流量存在突发且突发数据量超过分配的缓存最大值,则设备会对超过的报文进行丢包。因此,对于流量突发比较多且需要多个端口同时往一个端口发送流量的场景,请通过qos burst-mode enhanced命令设置缓存管理的突发模式为增强模式,以提高设备对突发流量的转发能力。

#### 表 11-3 设备缓存模式

缓存模式	说明	适用场景
标准模式	每个接口保留部分静态缓 存,突发时可以使用全局 的一小部分共享缓存。	适用于接口突发流量较小的场景。
增强模式	每个接口保留部分静态缓 存,突发时可以使用全局 的大部分共享缓存。	适用于接口突发流量较大的场景。
极限模式	每个接口保留部分静态缓 存,突发时可以使用全局 的极大部分共享缓存。	适用于接口突发流量极大的场景。

#### 操作步骤

- 配置设备缓存管理的突发模式。
  - a. 进入系统视图。

system-view

b. 配置缓存管理的突发模式。

对于S5732-H-V2、S6730-H-V2、S5735-S-V2、S5735I-S-V2、S5735I-H-V2、S5735I-L-V2、S5735-L-V2:

qos burst-mode enhanced slot slot-id

对于S5755-H:

qos burst-mode { enhanced | extreme } slot slot-id

- 配置接口缓存管理的突发模式。
  - a. 进入系统视图。

system-view

b. 进入接口视图。

interface { interface-type interface-number | interface-name }

c. 配置缓存管理的突发模式。

对于S5732-H-V2、S6730-H-V2、S5735-S-V2、S5735I-S-V2、S5735I-H-V2、S5735I-L-V2、S5735-L-V2:

qos burst-mode enhanced

对于S5755-H:

qos burst-mode { enhanced | extreme }

----结束

## 11.6.3 配置缓存空间的大小

#### 背景信息

当用户发现设备当前的缓存空间不能满足期望时,可以手工划分各缓存空间的大小。

#### 操作步骤

步骤1 进入系统视图。

system-view

步骤2 进入接口视图。

interface { interface-type interface-number | interface-name }

步骤3 配置队列级出方向的Queue Service缓存空间大小。

qos buffer queue queue-index shared-threshold dynamic dynamic-value

#### □□说明

执行该命令前,请确认系统视图下没有配置qos burst-mode(**系统视图)**命令,并且接口视图 下也没有配置qos burst-mode(**接口视图**)命令。

对于S5735I-L-V2、S5735I-S-V2、S5735-L-V2、S5735-S-V2、S5735I-H-V2系列,设备最多同时支持在28个接口下配置**qos buffer queue**命令。

----结束

## 11.6.4 配置队列缓存超限告警功能

#### 背景信息

设备的接口带宽大小是固定的,流量速率超过接口带宽且已使用的队列缓存超过配置的门限值时,设备会将超限的流量进行丢弃。通过配置命令qos buffer overrun threshold设置队列缓存超限告警阈值后,可以通过配置命令qos buffer overrun alarm enable使能队列缓存超限告警功能,当流量超过门限值时会产生告警。

#### 操作步骤

步骤1 进入系统视图。

system-view

步骤2 执行命令,配置队列缓存超限告警阈值。

qos buffer overrun threshold percent

步骤3 执行命令,使能队列缓存超限告警功能。

qos buffer overrun alarm enable

----结束

## 11.6.5 检查配置结果

#### 操作步骤

执行命令display qos buffer-usage [ slot slot-id | interface { interface-type interface-number | interface-name } ], 查看缓存使用情况。

#### ----结束

## 11.7 维护拥塞管理

#### 背景信息

#### 须知

清除统计信息后,以前的统计信息将无法恢复,务必仔细确认。

#### 操作步骤

- 清除基于队列的流量统计信息。
  reset qos queue statistics { interface { interface-type interface-number | interface-name } | slot slot-id }
- 清除缓存使用情况的统计数据。
  reset qos buffer-usage [ slot slot-id | interface { interface-type interface-number | interface-name } ]

#### ----结束

## 11.8 举例:配置拥塞管理

#### 组网需求

来自Host1和Host2的业务有语音、视频、数据,这些业务可经由DeviceB和DeviceA到达用户,为了减轻网络拥塞造成的影响,保证用户对于高优先级、低延迟业务的服务要求,配置需求如表11-4所述。

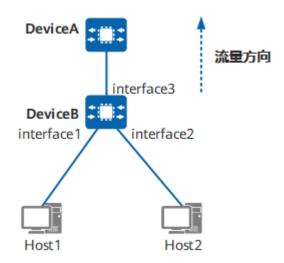
表 11-4 拥塞管理配置参数

业务类型	设备丢弃优先 级	设备内部优先 级	调度方式	调度权重
语音	绿	EF	PQ	-
视频	黄	AF3	WDRR	100
数据	红	AF1	WDRR	50

#### 图 11-4 拥塞管理配置组网图

#### 山 说明

本例中interface1, interface2, interface3分别代表10GE1/0/1, 10GE1/0/2和10GE1/0/3。



#### 操作步骤

#### 步骤1 配置各接口所属的VLAN,使各设备间链路互通

# 配置DeviceB接口10GE1/0/3的接口类型为trunk,并将接口10GE1/0/1加入 VLAN100,接口10GE1/0/2加入VLAN200,接口10GE1/0/3加入VLAN100和 VLAN200。仅S6730-H-V2系列、S5732-H-V2系列、S5755-H系列支持命令 **portswitch**。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] vlan batch 100 200
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] portswitch
[DeviceB-10GE1/0/1] port default vlan 100
[DeviceB-10GE1/0/1] quit
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] portswitch
[DeviceB-10GE1/0/2] port default vlan 200
[DeviceB-10GE1/0/2] quit
[DeviceB] interface 10ge 1/0/3
[DeviceB-10GE1/0/3] portswitch
[DeviceB-10GE1/0/3] port link-type trunk
[DeviceB-10GE1/0/3] port trunk allow-pass vlan 100 200
[DeviceB-10GE1/0/3] quit
```

**步骤2** 配置优先级映射,根据802.1p优先级将语音、数据、视频映射为不同的内部优先级, 实现对报文的分类。

# 创建DiffServ域ds1,将802.1p优先级6、5、2分别映射为设备内部优先级EF、AF3、AF1,并分别将丢弃优先级标记为绿色、黄色、红色。

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

# 在DeviceB入接口10GE1/0/1和10GE1/0/2上绑定DiffServ域。

```
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] trust 8021p outer
[DeviceB-10GE1/0/1] trust upstream ds1
[DeviceB-10GE1/0/1] quit
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] trust 8021p outer
```

```
[DeviceB-10GE1/0/2] trust upstream ds1
[DeviceB-10GE1/0/2] quit
```

**步骤3** 配置拥塞管理,通过配置各队列的调度参数,如调度方式和权重等,实现对不同优先级队列的差分调度。

#在DeviceB的报文出接口10GE1/0/3上配置各内部优先级对应队列的调度参数。

```
[DeviceB] interface 10ge 1/0/3
[DeviceB-10GE1/0/3] qos pq 5 to 7 drr 0 to 4
[DeviceB-10GE1/0/3] qos queue 3 drr weight 100
[DeviceB-10GE1/0/3] qos queue 1 drr weight 50
[DeviceB-10GE1/0/3] quit
[DeviceB] quit
```

#### ----结束

#### 检查配置结果

# 查看DiffServ域ds1的配置信息。

```
<DeviceB> display diffserv domain ds1
Diffserv domain name:ds1
8021p-inbound 0 phb be green
8021p-inbound 2 phb af1 green
8021p-inbound 3 phb af3 green
8021p-inbound 4 phb af4 green
8021p-inbound 5 phb af3 yellow
8021p-inbound 6 phb ef green
8021p-inbound 7 phb cs7 green
8021p-outbound be green map 0
8021p-outbound be yellow map 0
8021p-outbound be red map 0
8021p-outbound be red map 0
```

可以看到DiffServ域中将802.1p优先级6、5、2分别映射为设备内部优先级EF、AF3、AF1,并分别将丢弃优先级标记为绿色、黄色、红色。

# 查看接口10GE1/0/3的配置信息,可以看到各内部优先级对应队列的调度参数。

```
<DeviceB> display qos configuration interface 10ge 1/0/3
interface 10GE1/0/3
trust flag
            : outer 8021p
diffserv domain : default
dei enable
           : disable
port priority
             : 0
phb marking 8021p : disable
phb marking dscp: disable
phb marking exp :-
port wred
port lr
            : cir = -, cbs = -
port car inbound : -
port car outbound : -
schedule profile : -
           shaping
queue
                       schedule wred
       cir
             pir
       cbs
             pbs
0
              - drr
               - weight = 1
               - drr
               - weight = 50
      - - drr
```

#### 配置脚本

#### DeviceB的配置脚本

```
sysname DeviceB
vlan batch 100 200
diffserv domain ds1
8021p-inbound 2 phb af1 red
8021p-inbound 5 phb af3 yellow
8021p-inbound 6 phb ef green
interface 10GE1/0/1
port default vlan 100
trust upstream ds1
interface 10GE1/0/2
port default vlan 200
trust upstream ds1
interface 10GE1/0/3
port link-type trunk
port trunk allow-pass vlan 100 200
qos pq 5 to 7
qos queue 1 drr weight 50
qos queue 3 drr weight 100
return
```

## 11.9 举例:配置拥塞避免和拥塞管理综合示例(PQ+WDRR 调度和 WRED 模板)

#### 组网需求

DeviceB通过接口interface1与DeviceA互连,来自Internet的业务有语音、视频、数据,携带的802.1p优先级分别为6、5、2,这些业务可经由DeviceA和DeviceB到达用户,如图11-5所示。由于DeviceB入接口interface1的速率大于出接口interface2、interface3的速率,在这两个出接口处可能会发生拥塞。

为了减轻网络拥塞造成的影响,保证用户对于高优先级、低延迟业务的服务要求,配置需求如表11-5和表11-6所述。

表 11-5 拥塞避免配置参数

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

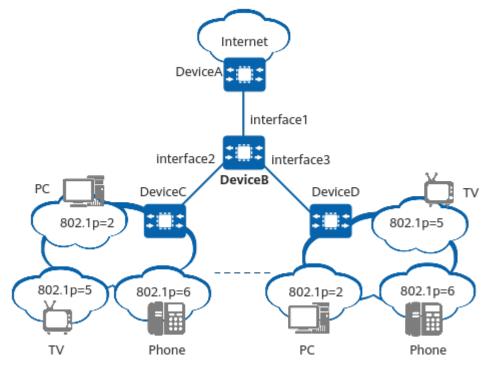
表 11-6 拥塞管理配置参数

业务类型	服务等级	WDRR
语音	EF	0
视频	AF3	100
数据	AF1	50

#### 图 11-5 拥塞避免和拥塞管理配置组网图

#### 山 说明

本例中interface1,interface2,interface3分别代表10GE1/0/1,10GE1/0/2和10GE1/0/3。



#### 操作步骤

步骤1 配置各接口所属的VLAN,使各设备间链路互通

仅S6730-H-V2系列、S5732-H-V2系列、S5755-H系列支持命令portswitch。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] vlan batch 2 5 6
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] portswitch
[DeviceB-10GE1/0/1] port link-type trunk
[DeviceB-10GE1/0/1] port trunk allow-pass vlan 2 5 6
DeviceB-10GE1/0/1] quit
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] portswitch
[DeviceB-10GE1/0/2] port link-type trunk
[DeviceB-10GE1/0/2] port trunk allow-pass vlan 2 5 6
[DeviceB-10GE1/0/2] quit
[DeviceB] interface 10ge 1/0/3
[DeviceB-10GE1/0/3] portswitch
[DeviceB-10GE1/0/3] port link-type trunk
[DeviceB-10GE1/0/3] port trunk allow-pass vlan 2 5 6
[DeviceB-10GE1/0/3] quit
```

**步骤2** 配置优先级映射,根据802.1p优先级将语音、数据、视频映射为不同的内部优先级, 实现对报文的分类。

# 创建DiffServ域ds1,将802.1p优先级6、5、2分别映射为设备内部优先级EF、AF3、AF1,并分别将丢弃优先级标记为绿色、黄色、红色。

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

#在DeviceB入接口10GE1/0/1上绑定DiffServ域。

```
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] trust 8021p inner
[DeviceB-10GE1/0/1] trust upstream ds1
[DeviceB-10GE1/0/1] quit
```

#### 步骤3 配置拥塞避免

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

#### [DeviceB] drop-profile wred1

[DeviceB-drop-wred1] **color green low-limit 80 high-limit 100 discard-percentage 10** //配置WRED丟弃模板,设置绿色报文丢弃上下限阈值和最大丢弃概率

[DeviceB-drop-wred1] **color yellow low-limit 60 high-limit 80 discard-percentage 20** //配置黄色报文占队列长度百分比为60%时开始丢弃报文,丢弃概率为20%,黄色报文占队列长度百分比达到80%时开始丢弃所有新到达报文

[DeviceB-drop-wred1] color red low-limit 40 high-limit 60 discard-percentage 40 [DeviceB-drop-wred1] quit

# 在DeviceB出接口10GE1/0/2、10GE1/0/3上应用WRED模板wred1。

```
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] qos queue 5 wred wred1
[DeviceB-10GE1/0/2] qos queue 3 wred wred1
[DeviceB-10GE1/0/2] qos queue 1 wred wred1
[DeviceB-10GE1/0/2] quit
[DeviceB] interface 10ge 1/0/3
[DeviceB-10GE1/0/3] qos queue 5 wred wred1
[DeviceB-10GE1/0/3] qos queue 3 wred wred1
[DeviceB-10GE1/0/3] qos queue 1 wred wred1
[DeviceB-10GE1/0/3] qos queue 1 wred wred1
[DeviceB-10GE1/0/3] quit
```

**步骤4** 配置拥塞管理,通过配置各队列的调度参数,如调度方式和权重等,实现对不同优先级队列的差分调度。

# 在DeviceB的报文出接口10GE1/0/2、10GE1/0/3上配置各服务等级队列的调度参数。

```
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] qos pq 5 to 7 drr 0 to 4 //配置5到7号队列为PQ调度,配置0到4号队列为WDRR调度
[DeviceB-10GE1/0/2] qos queue 3 drr weight 100 //配置3号队列的WDRR调度权值为100
[DeviceB-10GE1/0/2] qos queue 1 drr weight 50 //配置1号队列的WDRR调度权值为50,综上1号队列和3号队列中的报文按照1:2进行调度
[DeviceB-10GE1/0/2] quit
[DeviceB] interface 10ge 1/0/3
[DeviceB-10GE1/0/3] qos pq 5 to 7 drr 0 to 4 //配置5到7号队列为PQ调度,配置0到4号队列为WDRR调度
[DeviceB-10GE1/0/3] qos queue 3 drr weight 100
[DeviceB-10GE1/0/3] qos queue 1 drr weight 50
[DeviceB-10GE1/0/3] quit
[DeviceB] quit
```

#### ----结束

#### 检查配置结果

# 查看DiffServ域ds1的配置信息。

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

可以看到DiffServ域中将802.1p优先级6、5、2分别映射为设备内部优先级EF、AF3、AF1,并分别将丢弃优先级标记为绿色、黄色、红色。

# 查看WRED模板配置信息。

```
[DeviceB] display drop-profile wred1
Drop-profile[7]: wred1
      Mode Low-limit High-limit Unit Discard(%)
Color
Green Percentage 80
                        100
                               %
                                     10
Yellow Percentage 60
                               %
                        80
                                    20
Red Percentage 40
                       60
                              %
                                    40
```

#### 配置脚本

#### DeviceB的配置脚本

```
#
sysname DeviceB
#
vlan batch 2 5 to 6
#
diffserv domain ds1
8021p-inbound 2 phb af1 red
8021p-inbound 5 phb af3 yellow
8021p-inbound 6 phb ef green
#
drop-profile wred1
color green low-limit 80 high-limit 100 discard-percentage 10
```

```
color yellow low-limit 60 high-limit 80 discard-percentage 20
color red low-limit 40 high-limit 60 discard-percentage 40
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 2 5 to 6
qos pq 5 to 7 drr 0 to 4
qos queue 1 drr weight 50
qos queue 3 drr weight 100
qos queue 1 wred wred1
gos queue 3 wred wred1
qos queue 5 wred wred1
interface 10GE1/0/3
port link-type trunk
port trunk allow-pass vlan 2 5 to 6
qos pq 5 to 7 drr 0 to 4
gos queue 1 drr weight 50
qos queue 3 drr weight 100
qos queue 1 wred wred1
gos queue 3 wred wred1
gos queue 5 wred wred1
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 2 5 to 6
trust upstream ds1
trust 8021p inner
return
```

## 11.10 微突发检测

#### □ 说明

该功能仅S6730-H-V2、S5732-H-V2和S5755-H系列支持。

## 11.10.1 配置微突发检测

#### 背景信息

微突发是指接口在极短时间(毫秒级别)内收到大量突发流量,以至于瞬时速率达到平均速率的数十倍、数百倍,甚至超过接口带宽的现象。当微突发流量的瞬时速率超过设备的转发能力时,设备会将突发的数据进行缓存以便稍后发送。如果设备没有足够的缓存,那么超出的数据只能丢弃,这种现象就是拥塞丢包。在发生接口出方向拥塞丢包后,传统的问题定位方法较为困难和繁琐,通常是获取出方向报文,提取流量趋势,从而找到突发流量的特征。微突发检测功能可用于检测在极短时间内(毫秒级别)接口出方向的突发流量,便于维护人员确认是否是微突发引起丢包。通过检测微突发流量,既可以在拥塞发生前识别潜在的拥塞风险,也可以在拥塞发生后快速定位异常流量。

#### 微突发检测支持两种模式:

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

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

微突发检测的关键性能指标包括:

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

#### □ 说明

该功能仅S6730-H-V2、S5732-H-V2和S5755-H系列支持。

#### 操作步骤

- 配置设备的微突发检测功能
  - a. 进入系统视图

system-view

- b. 配置使能微突发检测模式 qos micro-burst detection [ enhanced ] enable
- 配置接口的微突发检测功能
  - a. 进入系统视图

system-view

b. 进入接口视图 interface { interface-type interface-number | interface-name }

c. 配置使能接口的微突发检测功能 gos micro-burst detection enable

## 11.10.2 检查配置结果

设备上使微突发检测功能后,查看设备的突发及丢包情况.

- 查看接口的微突发检测统计数据。
  display qos micro-burst statistics interface { interface-name | interface-type interface-number }
- 查看所有使能微突发检测的接口及接口的丢包情况。 display qos micro-burst status all
- 查看接口的缓存峰值和接口队列的缓存占用情况。
  display qos micro-burst peak-buffer verbose interface { interface-name | interface-type interface-number }

# 12 MPLS QoS 配置

- 12.1 MPLS QoS简介
- 12.2 MPLS QoS原理描述
- 12.3 MPLS QoS配置注意事项
- 12.4 MPLS QoS缺省配置
- 12.5 配置DiffServ模式
- 12.6 配置优先级映射
- 12.7 检查MPLS QoS配置结果
- 12.8 举例: 配置MPLS QoS示例

## 12.1 MPLS QoS 简介

#### 定义

MPLS QoS是一种特定的QoS业务,指在MPLS组网方案中通过差分服务(DiffServ)模型来实施QoS的技术。它可以为每个通过MPLS网络的业务提供指定的服务,并提供差异化的服务类型来满足各种需求。

#### 目的

MPLS使用标签转发替代了传统的路由转发,功能强大、灵活,可以满足各种新应用对网络的要求,而且MPLS支持多种网络协议(如IPv4、IPv6等)。目前MPLS被广泛地应用于大规模网络的组建,而在MPLS网络中,无法通过IP QoS来实现服务质量(QoS),所以在MPLS网络中实现服务质量也就应运而生,即MPLS QoS。

与传统IP QoS根据IP报文的优先级来区分业务的服务等级类似,MPLS QoS根据报文的 EXP来区分不同的数据流,实现差分服务,保证语音、视频数据流的低延时、低丢包率,保证网络的高利用率。

## 12.2 MPLS QoS 原理描述

在MPLS网络内部,MPLS QoS由MPLS报文首部的EXP字段区分数据流,提供差分服务,即E-LSP方案。在报文进入MPLS网络或从MPLS网络离开进入IP网络时,用户需要对是否信任报文初始携带的IP Precedence、DSCP、802.1p或EXP值做出选择。基于此,相关标准中定义了MPLS DiffServ的三种隧道模式: Uniform、Pipe和Short Pipe。

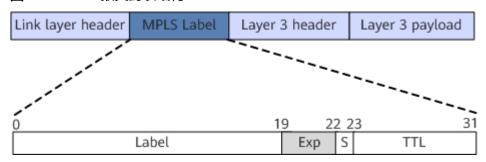
#### E-LSP 方案

IP QoS实现差分服务的方式是在网络的边缘进行流量分类,将流量划分为多个优先级或多个服务类,若使用IP报文头的IP Precedence来标记报文,可以将报文最多分成8类;若使用DSCP,则最多可分成64类。在报文发送途径中的每一跳通过检查报文的IP Precedence或DSCP字段,确定该数据包要求的QoS。

而在MPLS网络中,设备不会检查IP报文头的内容,因此无法通过IP Precedence或 DSCP字段来进行流量分类。目前设备采用E-LSP方案实现MPLS网络的流量分类。

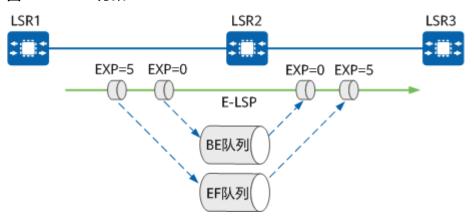
如<mark>图12-1</mark>,E-LSP方案使用MPLS报文首部的EXP字段来承载差分服务信息。转发时根据报文标签转发,由EXP决定对报文实施调度、监管等转发行为,即PHB(Per-Hop Behavior)。EXP可以从承载在LSP中的IP数据包的DSCP或IP Precedence拷贝,也可以由用户配置。

#### 图 12-1 MPLS 报文封装结构



如<mark>图12-2</mark>所示,在MPLS报文进设备LSR2时进行流分类,将报文携带的EXP统一映射到设备内部的服务等级和丢弃优先级。流量分类后,流量整形、流量监管、拥塞避免等QoS实现方法就和IP网络中的完全相同了。在报文出设备LSR2时,保留报文携带的EXP。

图 12-2 E-LSP 方案



#### MPLS DiffServ 隧道模式

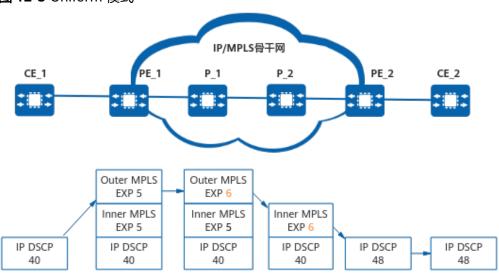
差分服务体系结构允许差分域内的中间节点检查并修改IP Precedence、DSCP、802.1p或EXP值,统称COS(Class of Service)值,这会导致报文的COS值在IP网络和MPLS网络传输过程中的都可能发生变化。因此,在报文进入MPLS网络或从MPLS网络离开进入IP网络时,用户需要在MPLS边缘路由器对COS(Class of Service)处理做出选择:是否信任IP/MPLS报文已经携带的COS信息。相关标准中定义了MPLS差分服务的三种隧道模式:Uniform、Pipe和Short Pipe。

#### ● Uniform模式:

当用户认为可以完全信任IP网络流量携带过来的COS(IP Precedence/DSCP/802.1p)时,可以采用Uniform模式: MPLS入节点将报文携带上来的COS直接复制到MPLS外层标签的EXP字段中,从而保证在MPLS中给予同样的QoS保证。报文离开MPLS网络时,出节点再将EXP字段值映射到IP报文的IP Precedence/DSCP/802.1p。

如<mark>图12-3</mark>所示,以L3VPN为例,在PE\_1上将报文的IP DSCP值映射为Outer MPLS EXP和Inner MPLS EXP值(为5),在P\_1上将Outer MPLS EXP值改为6,在P\_2上将外层MPLS标签弹出并将Inner MPLS EXP值置为Outer MPLS EXP值,在PE\_2上通过映射关系将报文的IP DSCP值变为了48。

图 12-3 Uniform 模式



Uniform模式,顾名思义,报文在IP网和MPLS网中的优先级标识是统一的,即报文进入MPLS域和出MPLS域都作优先级映射。但这样做的缺点是,如果报文在MPLS网络中改变了EXP字段的值,会导致报文离开MPLS网络后采用的PHB也发生改变,无法保留报文初始携带的COS值。

如<mark>图12-4</mark>所示,这两个Site属于同一企业的不同分部,企业网络中存在语音、数据和视频等多种业务流,已在企业网络中对三类业务区分优先级,保证语音优先级最高、视频其次、数据优先级最低。当不同VPN业务流量进入MPLS网络时,需要在MPLS网络中对三类业务区分优先级,保证MPLS网络中语音优先级一直最高、视频其次、数据优先级最低,并根据优先级的高低对三类业务提供不同的QoS服务。此时可以信任原报文携带的优先级,因此采用Uniform模式。

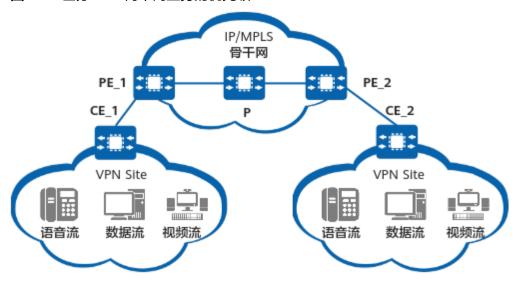


图 12-4 区分 VPN 内不同业务的优先级

## ● Pipe模式:

当用户认为IP网络流量携带过来的COS不可信任时,可以采用Pipe模式:忽略报文原来携带的COS,在MPLS域入节点可以为MPLS外层标签的EXP字段重新赋值,从MPLS入节点到出节点,流量都按照用户的意愿进行QoS调度,直到流量出MPLS域之后再根据其原来携带的COS值转发。

如<mark>图12-5</mark>所示,以L3VPN为例,在PE\_1上分别将Outer MPLS EXP和Inner MPLS EXP值置为1和2;在P\_2上将外层MPLS标签弹出并将Inner MPLS EXP值置为Outer MPLS EXP值;在PE\_2上并不改变原报文的IP DSCP值,报文根据Inner MPLS EXP值选择PHB。

图 12-5 Pipe 模式



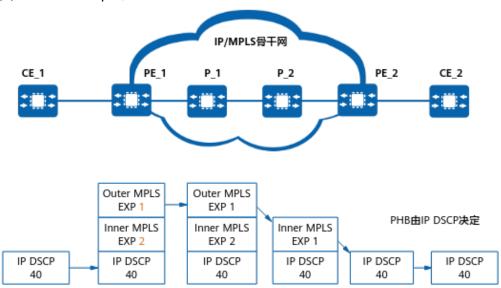
在Pipe模式中,报文在进入MPLS域时,入节点不拷贝IP Precedence/DSCP/802.1p到EXP。报文出MPLS域时,出节点也不拷贝EXP到IP Precedence/DSCP/802.1p。如果报文在MPLS网络中改变了EXP字段的值,只在MPLS网络中有效。当报文离开MPLS网络后,报文之前携带的COS继续有效。

#### • Short Pipe模式:

Short Pipe模式是对Pipe模式的改进,报文在MPLS入节点的处理和Pipe模式相同,但在MPLS网络的出节点上,出节点先执行标签弹出操作,再进行QoS调度。即,在MPLS出节点上按照报文之前携带的初始的COS值进行调度,而从报文进入MPLS开始到MPLS倒数第二跳按照用户的意愿进行QoS调度。

如<mark>图12-6</mark>所示,以L3VPN为例,在PE\_1上分别将Outer MPLS EXP和Inner MPLS EXP值置为1和2;在P\_2上将外层MPLS标签弹出并将Inner MPLS EXP值置为Outer MPLS EXP值;在PE\_2上并不改变原报文的IP DSCP值,报文IP DSCP值选择PHB。

图 12-6 Short Pipe 模式



使用Pipe或Short Pipe模式,在用户内部网络,用户可以根据自己的自身情况来规划QoS,而不改变客户侧的QoS。

Pipe模式和Short Pipe模式的区别在于: PE\_2上CE侧出方向的QoS调度, Pipe模式用户用自己的QoS标记, Short Pipe则采用客户侧的QoS标记。

如<mark>图12-7</mark>所示,CE\_1和CE\_3属于VPN\_1,并分别连接企业A的两个分部;CE\_2和CE\_4属于VPN\_2,并分别连接企业B的两个分部。当不同企业VPN业务进入MPLS网络时,需要在MPLS网络中对不同企业VPN区分优先级,保证企业A的优先级高、企业B的优先级低,并根据优先级的高低对不同企业提供不同的QoS服务。此时需要用户在报文进入MPLS网络时指定不同VPN下报文的EXP值,因此采用Pipe或Short pipe。

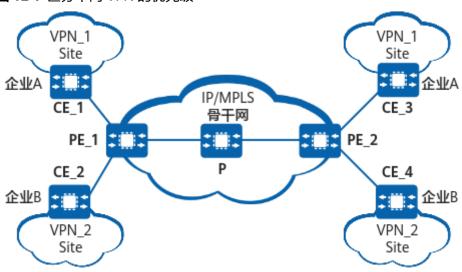


图 12-7 区分不同 VPN 的优先级

表 12-1 三种隧道模式的比较

隧道模式	入节点是否信任IP报 文原来携带的COS	出节点信任 EXP还是IP报 文原来携带的 COS	出节点QoS调 度行为	IP报文 原来携 带的 COS是 否会改	适用场 景
Uni for m	信任,将IP报文原来 携带的COS直接复制 到MPLS外层标签的 EXP字段	信任EXP,将 EXP字段值映 射到IP报文的 COS	根据EXP映射进 行调度	是	区分 VPN内 不同业 务的优 先级
Pip e	不信任,可以为 MPLS外层标签的EXP 字段重新赋值	信任IP报文原 来携带的 COS,保留报 文初始COS	根据EXP映射进 行调度	否	区分不 同VPN 的优先 级
Sh ort Pip e	不信任,可以为 MPLS外层标签的EXP 字段重新赋值	信任IP报文原 来携带的 COS,保留报 文初始COS	根据报文原来 携带的COS映 射进行调度	否	

# 12.3 MPLS QoS 配置注意事项

# License 依赖

MPLS QoS无需License许可即可使用。

# 硬件依赖

表 12-2 支持本特性的硬件

系列	支持产品
S5732-H-V2 series	S5732-H24S4X6QZ-V2/S5732-H24UM4Y2CZ-KV2/ S5732-H24UM4Y2CZ-V2/S5732-H44S4X6QZ-V2/ S5732-H48UM4Y2CZ-KV2/S5732-H48UM4Y2CZ- V2
S5755-H series	S5755-H24N4Y-A/S5755-H24P4Y2CZ/S5755- H24T4Y2CZ/S5755-H24U4Y2CZ/S5755- H24UN4Y2CZ/S5755-H24UTM4X4Y2C/S5755- H48N4Y-A/S5755-H48P4Y2CZ/S5755-H48T4Y2CZ/ S5755-H48U4Y2CZ/S5755-H48UN4Y2CZ/S5755- H48UTM4X4Y2C
S6730-H-V2 series	S6730-H24X6C-V2/S6730-H28X6CZ-V2/S6730- H48X6C-V2/S6730-H48X6CZ-V2/S6730-H48Y6C- V2

# 特性限制

无

# 12.4 MPLS QoS 缺省配置

报文进入设备时,报文的EXP值与设备PHB行为/颜色的缺省映射关系如表12-3所示。

表 12-3 入方向上 EXP 值与设备 PHB 行为/颜色的缺省映射关系

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

报文离开设备时,设备PHB行为/颜色与EXP值的缺省映射关系如表12-4所示。

表 12-4 出方向上设备 PHB 行为/颜色与 EXP 值的缺省映射关系

PHB行为	颜色	EXP值
BE	green	0
BE	yellow	0
BE	red	0
AF1	green	1
AF1	yellow	1
AF1	red	1
AF2	green	2
AF2	yellow	2
AF2	red	2
AF3	green	3
AF3	yellow	3
AF3	red	3
AF4	green	4
AF4	yellow	4
AF4	red	4
EF	green	5
EF	yellow	5
EF	red	5
CS6	green	6
CS6	yellow	6
CS6	red	6
CS7	green	7
CS7	yellow	7
CS7	red	7

# 12.5 配置 DiffServ 模式

# 前提条件

在配置DiffServ模式之前,需完成以下任务:

- 完成MPLS的基本组网配置。
- 配置VPN业务。

## 背景信息

MPLS DiffServ有三种隧道模式: Uniform、Pipe和Short Pipe。

- Uniform模式在报文进入MPLS网络时信任报文原来携带的优先级,适用于在VPN内区分不同业务的优先级。
- Pipe或Short pipe模式在报文进入MPLS网络时用户可以指定私网标签的EXP值,适用于区分不同VPN之间的优先级。

用户希望不改变原报文携带的优先级时,建议使用Pipe或Short pipe模式,因为 Uniform模式可能会改变原报文携带的优先级。另外,Uniform和Pipe模式在Egress上 根据报文的EXP优先级选择PHB,而Short pipe模式根据报文的DSCP优先级选择PHB。

# 操作步骤

步骤1 进入系统视图。

system-view

步骤2 进入VPN实例视图。

ip vpn-instance vpn-instance-name

步骤3 选择一种类型进入地址族视图。

- 进入IPv4地址族视图。 ipv4-family
- 进入IPv6地址族视图。ipv6-family

#### 步骤4 配置VPN实例的差分服务模式。

diffserv-mode { pipe { mpls-exp exp-value | domain ds-name } | short-pipe [ mpls-exp exp-value ]
domain ds-name | uniform [ domain ds-name ] }

缺省情况下,VPN实例的差分服务模式为Uniform模式,使用default域。

#### □ 说明

- Diffserv模式只能在PE节点应用。
- 配置diffserv-mode { pipe { mpls-exp exp-value | domain ds-name } | short-pipe [ mpls-exp exp-value ] domain ds-name }命令,指定exp-value后,MPLS私网标签的exp会设置成该值。

----结束

# 12.6 配置优先级映射

# 背景信息

优先级映射功能的配置逻辑如下:

1. 配置DiffServ域:配置DiffServ域可以确定EXP值与内部优先级的映射关系,以便设备根据内部优先级提供有差别的QoS服务。

2. 应用DiffServ域:将DiffServ域应用在对象上,使DiffServ域中的映射关系生效。

# 12.6.1 配置 DiffServ 域

# 背景信息

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

# 操作步骤

步骤1 进入系统视图。

system-view

步骤2 创建DiffServ域并进入DiffServ域视图。

diffserv domain ds-domain-name

缺省情况下存在default域,支持修改,但不能删除。缺省优先级映射关系请参见 "MPLS QoS缺省配置"的表12-3和表12-4。

用户也可以创建新的Diffserv域,并定义优先级映射关系。

步骤3 请根据实际情况对设备的优先级映射进行定义。

- 在接口入方向,将MPLS报文的EXP优先级映射为PHB行为/颜色。 mpls-exp-inbound exp-value phb service-class color
- 在接口出方向,将报文的PHB行为/颜色映射为MPLS报文中EXP优先级。 mpls-exp-outbound service-class color map exp-value

----结束

# 12.6.2 应用 DiffServ 域

# 背景信息

当需要根据DiffServ域中定义的映射关系,对流入设备的报文进行优先级到PHB行为和 颜色之间的映射操作时,可以将DiffServ域绑定到报文的入接口,系统会根据DiffServ 域中的映射关系将报文的优先级映射为相应的PHB行为和颜色。

当需要根据DiffServ域中定义的映射关系,对流出设备的报文进行PHB行为到优先级之间的映射操作时,可以将DiffServ域绑定到报文的出接口,系统会根据DiffServ域中的映射关系将报文的PHB行为和颜色映射为优先级。

## 山 说明

- 当全局MPLS未使能时,不存在缺省配置,该功能不生效。
- 当全局MPLS使能后,存在缺省配置。必须在公网隧道建立之前配置该功能才会生效。
- 如果在公网隧道建立之后配置该功能,并且需要其立即生效,则须重启MPLS LDP会话。
- 更改全局指定的DS域,或者更改接口、VSI、VPN实例下的diffserv模式后,如果需要其立即 生效,则须重新建立MPLS LDP会话。

# 操作步骤

- 在Ingress设备上配置公网隧道基于EXP进行优先级映射。
  - a. 进入系统视图。

#### system-view

- b. 在Ingress设备上配置公网隧道基于EXP进行优先级映射。
  mpls-qos ingress { use vpn-label-exp | trust upstream { ds-name | default | none } }
  缺省情况下,根据默认的default域进行公网隧道的EXP的优先级映射。
- 在Transit设备上配置公网隧道基于EXP进行优先级映射。
  - a. 进入系统视图。

system-view

b. 在Transit设备上配置公网隧道基于EXP进行优先级映射。 mpls-qos transit trust upstream { none | default | *ds-name* }

缺省情况下,根据默认的default域进行公网隧道的EXP的优先级映射。

- 在Egress设备上配置公网隧道基于EXP进行优先级映射。
  - a. 进入系统视图。

system-view

b. 在Egress设备上配置公网隧道基于EXP进行优先级映射。 mpls-qos egress trust upstream { none | default | *ds-name* }

缺省情况下,根据默认的default域进行公网隧道的EXP的优先级映射。

#### ----结束

# 12.7 检查 MPLS QoS 配置结果

## 操作步骤

- 执行命令**display diffserv domain** [ **brief** | *ds-domain-name* ],查看DiffServ域的配置信息。
- 执行命令**display qos configuration interface** [ *interface-type interface-number* ],查看接口上所有的QoS配置信息。

#### ----结束

# 12.8 举例: 配置 MPLS QoS 示例

## 组网需求

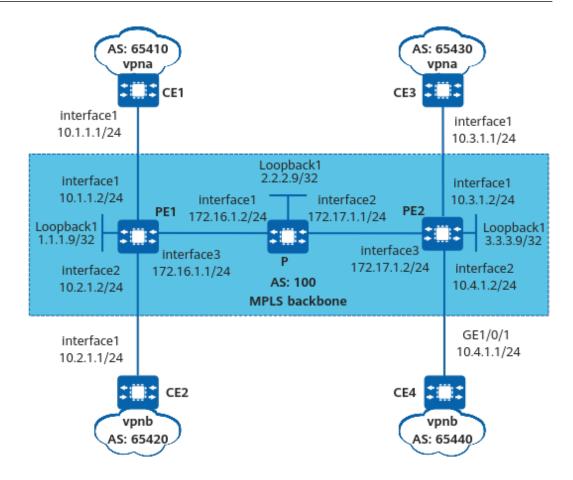
企业A和企业B通过部署BGP/MPLS IP VPN,实现总部和分支机构的互联。如<mark>图12-8</mark>,CE1、CE3连接企业A的总部和分支,CE2、CE4连接企业B的总部和分支。企业A使用vpna,企业B使用vpnb。

由于企业A的服务等级高,要求给企业A提供更好的QoS保证。

#### 图 12-8 MPLS QoS 模式组网

#### □ 说明

本例中interface1, interface2, interface3分别代表1/0/1, 1/0/2, 1/0/3。



# 配置思路

在PE1和PE2上配置MPLS QoS,将vpna和vpnb分别使能Pipe模式,vpna和vpnb的mpls-exp值分别设置为4和3,实现对企业A的业务提供更好的QoS保证。

# 操作步骤

步骤1 在MPLS骨干网上配置OSPF协议,实现骨干网PE和P的互通。

## # 配置PE1。

```
<HUAWEI> system-view
[HUAWEI] sysname PE1
[PE1] interface loopback 1
[PE1-LoopBack1] ip address 1.1.1.9 32
[PE1-LoopBack1] quit
[PE1] interface 10ge 1/0/3
[PE1-10GE1/0/3] ip address 172.16.1.1 24
[PE1-10GE1/0/3] quit
[PE1] ospf 1
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 172.16.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

#### # 配置P。

```
<HUAWEI> system-view
[HUAWEI] sysname P
[P] interface loopback 1
[P-LoopBack1] ip address 2.2.2.9 32
```

```
[P-LoopBack1] quit
[P] interface 10ge 1/0/1
[P-10GE1/0/1] ip address 172.16.1.2 24
[P-10GE1/0/1] quit
[P] interface 10ge 1/0/2
[P-10GE1/0/2] ip address 172.17.1.1 24
[P-10GE1/0/2] quit
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 172.16.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 172.17.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

#### # 配置PE2。

```
<HUAWEI> system-view
[HUAWEI] sysname PE2
[PE2] interface loopback 1
[PE2-LoopBack1] ip address 3.3.3.9 32
[PE2-LoopBack1] quit
[PE2] interface 10ge 1/0/3
[PE2-10GE1/0/3] ip address 172.17.1.2 24
[PE2-10GE1/0/3] quit
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 172.17.1.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE2-ospf-1] quit
```

配置完成后,PE1、P、PE2之间应能建立OSPF邻居关系,执行display ip routing-table命令可以看到PE之间学习到对方的Loopback1路由。

#### 步骤2 在MPLS骨干网上配置MPLS基本能力和MPLS LDP, 建立LDP LSP

## # 配置PE1。

```
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] interface 10ge 1/0/3
[PE1-10GE1/0/3] mpls
[PE1-10GE1/0/3] quit
```

## # 配置P。

```
[P] mpls lsr-id 2.2.2.9
[P] mpls
[P-mpls] quit
[P] mpls ldp
[P-mpls-ldp] quit
[P] interface 10ge 1/0/1
[P-10GE1/0/1] mpls
[P-10GE1/0/1] quit
[P] interface 10ge 1/0/2
[P-10GE1/0/2] mpls ldp
[P-10GE1/0/2] mpls
[P-10GE1/0/2] mpls ldp
[P-10GE1/0/2] mpls ldp
[P-10GE1/0/2] quit
```

## # 配置PE2。

```
[PE2] mpls lsr-id 3.3.3.9
[PE2] mpls
```

```
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
[PE2] interface 10ge 1/0/3
[PE2-10GE1/0/3] mpls
[PE2-10GE1/0/3] mpls ldp
[PE2-10GE1/0/3] quit
```

上述配置完成后,PE1与P、P与PE2之间应能建立LDP会话,执行**display mpls ldp session**命令可以看到显示结果中Status项为"Operational"。

#### 以PE1的显示为例:

#### 步骤3 在PE设备上配置VPN实例,将CE接入PE

#### # 配置PE1。

```
[PE1] ip vpn-instance vpna
[PE1-vpn-instance-vpna] ipv4-family
[PE1-vpn-instance-vpna-af-ipv4] route-distinguisher 100:1
[PE1-vpn-instance-vpna-af-ipv4] vpn-target 111:1 both
[PE1-vpn-instance-vpna-af-ipv4] quit
[PE1-vpn-instance-vpna] quit
[PE1] ip vpn-instance vpnb
[PE1-vpn-instance-vpnb] ipv4-family
[PE1-vpn-instance-vpnb-af-ipv4] route-distinguisher 100:2
[PE1-vpn-instance-vpnb-af-ipv4] vpn-target 222:2 both
[PE1-vpn-instance-vpnb-af-ipv4] quit
[PE1-vpn-instance-vpnb] quit
[PE1] interface 10ge 1/0/1
[PE1-10GE1/0/1] ip binding vpn-instance vpna
[PE1-10GE1/0/1] ip address 10.1.1.2 24
[PE1-10GE1/0/1] quit
[PE1] interface 10ge 1/0/2
[PE1-10GE1/0/2] ip binding vpn-instance vpnb
[PE1-10GE1/0/2] ip address 10.2.1.2 24
[PE1-10GE1/0/2] quit
```

## # 配置PE2。

```
[PE2] ip vpn-instance vpna
[PE2-vpn-instance-vpna] ipv4-family
[PE2-vpn-instance-vpna-af-ipv4] route-distinguisher 200:1
[PE2-vpn-instance-vpna-af-ipv4] vpn-target 111:1 both
[PE2-vpn-instance-vpna-af-ipv4] quit
[PE2-vpn-instance-vpna] quit
[PE2] ip vpn-instance vpnb
[PE2-vpn-instance-vpnb] ipv4-family
[PE2-vpn-instance-vpnb-af-ipv4] route-distinguisher 200:2
[PE2-vpn-instance-vpnb-af-ipv4] vpn-target 222:2 both
[PE2-vpn-instance-vpnb-af-ipv4] quit
[PE2-vpn-instance-vpnb] quit
[PE2] interface 10ge 1/0/1
[PE2-10GE1/0/1] ip binding vpn-instance vpna
[PE2-10GE1/0/1] ip address 10.3.1.2 24
[PE2-10GE1/0/1] quit
[PE2] interface 10ge 1/0/2
[PE2-10GE1/0/2] ip binding vpn-instance vpnb
[PE2-10GE1/0/2] ip address 10.4.1.2 24
[PE2-10GE1/0/2] quit
```

#按图12-8配置各CE的接口IP地址,配置过程略。

配置完成后,各PE能Ping通自己接入的CE。

#### □ 说明

当PE上有多个绑定了同一个VPN的接口,则使用**ping -vpn-instance**命令Ping对端PE接入的CE 时,要指定源IP地址,即要指定**ping -vpn-instance** *vpn-instance-name* **-a** *source-ip-address* 命令中的参数**-a** *source-ip-address*,否则可能Ping不通。

#### 以PE1和CE1为例:

```
[PE1] ping -vpn-instance vpna 10.1.1.1

PING 10.1.1.1: 56 data bytes, press CTRL_C to break

Reply from 10.1.1.1: bytes=56 Sequence=1 ttl=255 time=5 ms

Reply from 10.1.1.1: bytes=56 Sequence=2 ttl=255 time=3 ms

Reply from 10.1.1.1: bytes=56 Sequence=3 ttl=255 time=3 ms

Reply from 10.1.1.1: bytes=56 Sequence=4 ttl=255 time=3 ms

Reply from 10.1.1.1: bytes=56 Sequence=5 ttl=255 time=16 ms

--- 10.1.1.1 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 3/6/16 ms
```

#### 步骤4 在PE之间建立MP-IBGP对等体关系

#### # 配置PE1。

```
[PE1] bgp 100
[PE1-bgp] peer 3.3.3.9 as-number 100
[PE1-bgp] peer 3.3.3.9 connect-interface loopback 1
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpnv4] peer 3.3.3.9 enable
[PE1-bgp-af-vpnv4] quit
[PE1-bgp] quit
```

#### # 配置PE2。

```
[PE2] bgp 100
[PE2-bgp] peer 1.1.1.9 as-number 100
[PE2-bgp] peer 1.1.1.9 connect-interface loopback 1
[PE2-bgp] ipv4-family vpnv4
[PE2-bgp-af-vpnv4] peer 1.1.1.9 enable
[PE2-bgp-af-vpnv4] quit
[PE2-bgp] quit
```

配置完成后,在PE设备上执行**display bgp peer**命令,可以看到PE之间的BGP对等体关系已建立,并达到Established状态。

```
[PE1] display bgp peer

BGP local router ID: 1.1.1.9
Local AS number: 100
Total number of peers: 1 Peers in established state: 1

Peer V AS MsgRcvd MsgSent OutQ Up/Down State PrefRcv

3.3.3.9 4 100 12 6 0 00:02:21 Established 0
```

## 步骤5 在PE与CE之间建立EBGP对等体关系,引入VPN路由

## # 配置CE1。

```
<HUAWEI> system-view
[HUAWEI] sysname CE1
[CE1] bgp 65410
```

```
[CE1-bgp] peer 10.1.1.2 as-number 100
[CE1-bgp] import-route direct
```

CE2、CE3、CE4配置与CE1设备配置类似,配置过程省略。

#### # 配置PE1。

```
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpna
[PE1-bgp-vpna] peer 10.1.1.1 as-number 65410
[PE1-bgp-vpna] import-route direct
[PE1-bgp-vpna] quit
[PE1-bgp] ipv4-family vpn-instance vpnb
[PE1-bgp-vpnb] peer 10.2.1.1 as-number 65420
[PE1-bgp-vpnb] import-route direct
[PE1-bgp-vpnb] quit
[PE1-bgp] quit
```

PE2的配置与PE1类似,配置过程省略。

配置完成后,在PE设备上执行**display bgp vpnv4 vpn-instance peer**命令,可以看到PE与CE之间的BGP对等体关系已建立,并达到Established状态。

以PE1与CE1的对等体关系为例:

```
[PE1] display bgp vpnv4 vpn-instance vpna peer

BGP local router ID : 1.1.1.9
Local AS number : 100
Total number of peers : 1 Peers in established state : 1

Peer V AS MsgRcvd MsgSent OutQ Up/Down State PrefRcv

10.1.1.1 4 65410 11 9 0 00:07:25 Established 1
```

#### 步骤6 配置DiffServ模式。

## #配置PE1。

```
[PE1] mpls-qos ingress use vpn-label-exp
[PE1] ip vpn-instance vpna
[PE1-vpn-instance-vpna] ipv4-family
[PE1-vpn-instance-vpna-af-ipv4] diffserv-mode pipe mpls-exp 4
[PE1-vpn-instance-vpna-af-ipv4] quit
[PE1-vpn-instance-vpna] quit
[PE1] ip vpn-instance vpnb
[PE1-vpn-instance-vpnb] ipv4-family
[PE1-vpn-instance-vpnb-af-ipv4] diffserv-mode pipe mpls-exp 3
[PE1-vpn-instance-vpnb-af-ipv4] quit
[PE1-vpn-instance-vpnb] quit
```

#### #配置PE2。

```
[PE2] mpls-qos ingress use vpn-label-exp
[PE2] ip vpn-instance vpna
[PE1-vpn-instance-vpna] ipv4-family
[PE2-vpn-instance-vpna-af-ipv4] diffserv-mode pipe mpls-exp 4
[PE2-vpn-instance-vpna-af-ipv4] quit
[PE1-vpn-instance-vpna] quit
[PE2] ip vpn-instance vpnb
[PE1-vpn-instance-vpnb] ipv4-family
[PE2-vpn-instance-vpnb-af-ipv4] diffserv-mode pipe mpls-exp 3
[PE2-vpn-instance-vpnb-af-ipv4] quit
[PE1-vpn-instance-vpnb] quit
```

## 步骤7

# 🗀 说明

配置完成后,需重启MPLS LDP和复位BGP连接,配置方能生效。

### ----结束

## 配置脚本

### ● PE1的配置脚本

```
sysname PE1
mpls-qos ingress use vpn-label-exp
ip vpn-instance vpna
ipv4-family
 route-distinguisher 100:1
 vpn-target 111:1 export-extcommunity
 vpn-target 111:1 import-extcommunity
 diffserv-mode pipe mpls-exp 4
ip vpn-instance vpnb
ipv4-family
 route-distinguisher 100:2
 vpn-target 222:2 export-extcommunity
 vpn-target 222:2 import-extcommunity
 diffserv-mode pipe mpls-exp 3
mpls lsr-id 1.1.1.9
mpls
mpls ldp
interface 10ge 1/0/1
ip binding vpn-instance vpna
ip address 10.1.1.2 255.255.255.0
interface 10ge 1/0/2
ip binding vpn-instance vpnb
ip address 10.2.1.2 255.255.255.0
interface 10ge 1/0/3
ip address 172.16.1.1 255.255.255.0
mpls
mpls ldp
interface LoopBack1
ip address 1.1.1.9 255.255.255.255
bgp 100
peer 3.3.3.9 as-number 100
peer 3.3.3.9 connect-interface LoopBack1
ipv4-family unicast
 undo synchronization
 peer 3.3.3.9 enable
ipv4-family vpnv4
 policy vpn-target
 peer 3.3.3.9 enable
ipv4-family vpn-instance vpna
 import-route direct
 peer 10.1.1.1 as-number 65410
ipv4-family vpn-instance vpnb
 import-route direct
 peer 10.2.1.1 as-number 65420
```

```
#
ospf 1
area 0.0.0.0
network 1.1.1.9 0.0.0.0
network 172.16.1.0 0.0.0.255
#
return
```

### ● P的配置脚本

```
sysname P
mpls lsr-id 2.2.2.9
mpls
mpls ldp
interface 10ge 1/0/1
ip address 172.16.1.2 255.255.255.0
mpls
mpls ldp
interface 10ge 1/0/2
ip address 172.17.1.1 255.255.255.0
mpls
mpls ldp
interface LoopBack1
ip address 2.2.2.9 255.255.255.255
ospf 1
area 0.0.0.0
 network 2.2.2.9 0.0.0.0
 network 172.16.1.0 0.0.0.255
 network 172.17.1.0 0.0.0.255
return
```

### ● PE2的配置脚本

```
sysname PE2
mpls-qos ingress use vpn-label-exp
ip vpn-instance vpna
ipv4-family
 route-distinguisher 200:1
 vpn-target 111:1 export-extcommunity
 vpn-target 111:1 import-extcommunity
 diffserv-mode pipe mpls-exp 4
ip vpn-instance vpnb
ipv4-family
 route-distinguisher 200:2
 vpn-target 222:2 export-extcommunity
 vpn-target 222:2 import-extcommunity
diffserv-mode pipe mpls-exp 3
mpls lsr-id 3.3.3.9
mpls
mpls ldp
interface 10ge 1/0/1
ip binding vpn-instance vpna
ip address 10.3.1.2 255.255.255.0
interface 10ge 1/0/2
ip binding vpn-instance vpnb
ip address 10.4.1.2 255.255.255.0
```

```
interface 10ge 1/0/3
ip address 172.17.1.2 255.255.255.0
mpls
mpls ldp
interface LoopBack1
ip address 3.3.3.9 255.255.255.255
peer 1.1.1.9 as-number 100
peer 1.1.1.9 connect-interface LoopBack1
ipv4-family unicast
 undo synchronization
 peer 1.1.1.9 enable
ipv4-family vpnv4
 policy vpn-target
 peer 1.1.1.9 enable
ipv4-family vpn-instance vpna
 import-route direct
 peer 10.3.1.1 as-number 65430
ipv4-family vpn-instance vpnb
 import-route direct
 peer 10.4.1.1 as-number 65440
ospf 1
area 0.0.0.0
 network 3.3.3.9 0.0.0.0
 network 172.17.1.0 0.0.0.255
return
```

#### ● 企业A总部出口处CE1的配置脚本

```
#
sysname CE1
#
interface 10ge 1/0/1
ip address 10.1.1.1 255.255.255.0
#
bgp 65410
peer 10.1.1.2 as-number 100
#
ipv4-family unicast
undo synchronization
import-route direct
peer 10.1.1.2 enable
#
return
```

### ● 企业B总部出口处CE2的配置脚本

```
# sysname CE2
# interface 10ge 1/0/1
ip address 10.2.1.1 255.255.255.0
# bgp 65420
peer 10.2.1.2 as-number 100
# ipv4-family unicast
undo synchronization
import-route direct
peer 10.2.1.2 enable
# return
```

## ● 企业A分支出口处CE3的配置脚本

```
#
sysname CE3
#
interface 10ge 1/0/1
ip address 10.3.1.1 255.255.255.0
#
bgp 65430
peer 10.3.1.2 as-number 100
#
ipv4-family unicast
undo synchronization
import-route direct
peer 10.3.1.2 enable
#
return
```

## ● 企业B分支出口处CE4的配置脚本

```
# sysname CE4
# vlan batch 50
# interface 10ge 1/0/1
ip address 10.4.1.1 255.255.255.0
# bgp 65440
peer 10.4.1.2 as-number 100
# ipv4-family unicast
undo synchronization
import-route direct
peer 10.4.1.2 enable
# return
```