目 录

1 QoS 配置

1.1 概述

QoS（Quality of Service，服务质量）用于评估服务方满足客户服务需求的能力。在 Internet 中，QoS 所评估的就是网络转发分组的服务能力。

由于网络提供的服务是多样的，因此 QoS 的评估可以基于不同方面。通常所说的 QoS，是对分组转发过程中带宽、延迟、抖动、丢包率等指标进行评估。

1.1.1 无 QoS 保障的网络

在传统的无 QoS 保障的 IP 网络中，设备无区别地对待所有的报文，设备处理报文采用的策略是 FIFO（First In First Out，先入先出），它依照报文到达时间的先后顺序分配转发所需要的资源。所有报文共享网络和设备的资源，至于得到资源的多少完全取决于报文到达的时间。这种服务策略称作 Best-Effort，它尽最大的努力将报文送到目的地，但对分组转发的延迟、抖动、丢包率等需求不提供任何承诺和保证。

传统的 Best-Effort 服务策略只适用于对带宽、延迟不敏感的 WWW、E-Mail 等业务。

1.1.2 新业务对 QoS 的需求

随着计算机网络的高速发展，越来越多的网络接入 Internet。无论从规模、覆盖范围还是用户数量上来看，Internet 都扩展得非常快。

除了传统的 WWW、E-Mail 应用外，用户还尝试在 Internet 上拓展新业务，比如远程教学、远程医疗、可视电话、电视会议、视频点播等。企业用户也希望通过 VPN 技术，将分布在各地的分支机构连接起来，开展一些事务性应用：比如访问公司的数据库或通过 Telnet 管理远程设备。

这些新业务有一个共同特点，即对带宽、延迟、抖动等传输性能有着特殊的需求。比如电视会议、视频点播需要高带宽、低延迟和低抖动的保证。事务处理、Telnet 等关键任务虽然不一定要求高带宽，但非常注重低延迟，在拥塞发生时要求优先获得处理。

新业务的不断涌现对 IP 网络的服务能力提出了更高的要求，用户已不再满足于能够简单地将报文送达目的地，还希望在转发过程中得到更好的服务，诸如为用户提供专用带宽、减少报文的丢失率、管理和避免网络拥塞、调控网络的流量。所有这些都要求网络具备更为完善的服务能力。

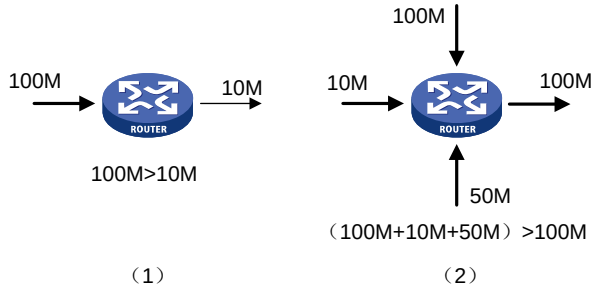
1.1.3 拥塞的产生、影响和对策

传统网络所面临的服务质量问题，主要是由网络拥塞引起的。所谓拥塞，是指由于供给资源的相对不足而造成转发速率下降、引入额外延迟，从而导致服务质量下降的一种现象。

1. 拥塞的产生

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

图1-1 流量拥塞示意图



(1) 分组流从高速链路进入设备，由低速链路转发出去。

(2) 分组流从多个接口同时进入网络设备，由一个接口转发出去（多个接口的速率和 〉 出接口的速率）。

如果流量以线速到达，那么就会遭遇资源的瓶颈而导致拥塞。

不仅仅是链路带宽的瓶颈会导致拥塞，任何用于正常转发处理的资源的不足（如可分配的处理器时间、缓冲区、内存资源的不足）都会造成拥塞。此外，在某个时间内对所到达的流量控制不力，使之超出了可分配的网络资源，也是引发网络拥塞的一个因素。

2. 拥塞的影响

拥塞有可能会引发一系列的负面影响：

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

可见，拥塞使流量不能及时获得资源是造成服务性能下降的源头。在分组交换以及多用户业务并存的复杂环境下，拥塞又是不可避免的，因此必须采用适当的方法来解决拥塞。

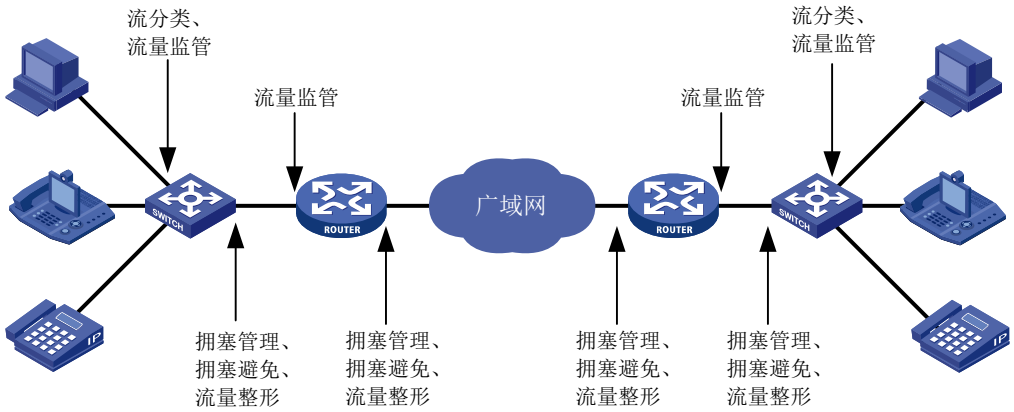
3. 对策

增加网络带宽是解决资源不足的一个直接途径，然而网络带宽不可能无限制的增加，因此它并不能解决所有导致网络拥塞的问题。

解决网络拥塞问题的一个更有效的办法是在网络中增加流量控制和资源分配的功能，为有不同服务需求的业务提供有差别的服务，更合理地分配和使用资源。在进行资源分配和流量控制的过程中，尽可能地控制好那些可能引发网络拥塞的直接或间接因素，从而减少拥塞发生的概率；在拥塞发生时，依据业务的性质及其需求权衡资源的分配，将拥塞的影响减到最小。

1.1.4 端到端的 QoS

图1-2 端到端 QoS 模型图



如上图所示，流分类、流量监管、流量整形、拥塞管理和拥塞避免是构造有区别地实施服务的基石，它们主要完成如下功能：

- 流分类：依据一定的匹配规则识别出报文，通常作用在接口入方向。
- 流量监管：对进入或流出设备的特定流量的规格进行监管。当流量超出规格时，可以采取限制或惩罚措施，以保护网络资源不受损害。可以作用在接口入方向和出方向。
- 流量整形：一种主动调整流的输出速率的流控措施，用来使流量适配下游设备可供给的网络资源，避免不必要的报文丢弃和拥塞，通常作用在接口出方向。
- 拥塞管理：就是当拥塞发生时如何制定一个资源的调度策略，以决定报文转发的处理次序，通常作用在接口出方向。
- 拥塞避免：监督网络资源的使用情况，当发现拥塞有加剧的趋势时采取主动丢弃报文的策略，通过调整流量来解除网络的过载，通常作用在接口出方向。

在这些 QoS 技术中，流分类是基础，是有区别地实施服务的前提；而流量监管、流量整形、拥塞管理和拥塞避免从不同方面对网络流量及其分配的资源实施控制，是有区别地提供服务思想的具体体现。

1.1.5 流分类技术

流分类可以使用 IP 报文头的 ToS（Type of Service，服务类型）字段的优先级位，识别出有不同优先级特征的流量；也可以由网络管理者设置流分类的策略，例如综合源地址、目的地址、MAC 地址、IP 协议或应用程序的端口号等信息对流进行分类。

流分类的结果是没有范围限制的，它可以是一个由五元组（源地址、源端口号、协议号、目的地址、目的端口号）确定的狭小范围，也可以是到某网段的所有报文。

一般在网络边界对报文分类时，同时设置报文 IP 头的 ToS 字段中的优先级位。这样，在网络的内部就可以直接使用 IP 优先级作为分类标准。而队列技术也可以使用这个优先级来对报文进行不同的处理。下游网络可以选择接收上游网络的分类结果，也可以按照自己的标准重新进行分类。

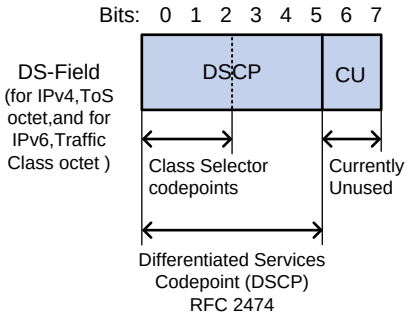
进行流分类是为了有区别地提供服务，它必须与某种流控或资源分配动作关联起来才有意义。具体采取何种流控动作，与所处的阶段以及网络当前的负载状况有关。例如，当报文进入网络时依据承

诺速率对它进行监管；流出节点之前进行整形；拥塞时对队列进行调度管理；拥塞加剧时采取拥塞避免措施等。

1.1.6 报文优先级

1. DSCP 优先级

图1-3 ToS 和 DS 域



如上图 1-3 所示，IP 报文头的 ToS 字段有 8 个 bit，RFC 2474 中，重新定义了 IP 报文头部的 ToS 域，称之为 DS（Differentiated Services，差分服务）域，其中 DSCP 优先级用该域的前 6 位（0～5 位）表示，取值范围为 0～63，后 2 位（6、7 位）是保留位。

表1-1 DSCP 优先级说明

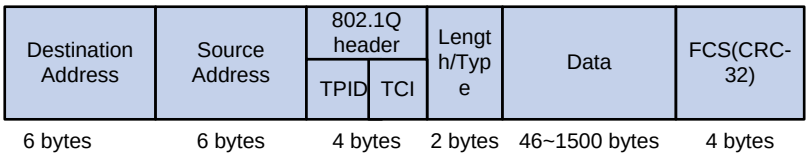
IP 优先级（十进制）	IP 优先级（二进制）	关键字
46	101110	ef
10	001010	af11
12	001100	af12
14	001110	af13
18	010010	af21
20	010100	af22
22	010110	af23
26	011010	af31
28	011100	af32
30	011110	af33
34	100010	af41
36	100100	af42
38	100110	af43
8	001000	cs1
16	010000	cs2
24	011000	cs3
32	100000	cs4

IP 优先级（十进制）	IP 优先级（二进制）	关键字
40	101000	cs5
48	110000	cs6
56	111000	cs7
0	000000	be（default）

2. 802.1p 优先级

802.1p 优先级位于二层报文头部，适用于不需要分析三层报头，而需要在二层环境下保证 QoS 的场合。

图1-4 带有 802.1Q 标签头的以太网帧



如上图所示，4 个字节的 802.1Q 标签头包含了 2 个字节的 TPID（Tag Protocol Identifier，标签协议标识符）和 2 个字节的 TCI（Tag Control Information，标签控制信息），TPID 取值为 0x8100。下图显示了 802.1Q 标签头的详细内容，Priority 字段就是 802.1p 优先级。之所以称此优先级为 802.1p 优先级，是因为有关这些优先级的应用是在 802.1p 规范中被详细定义的。

图1-5 802.1Q 标签头

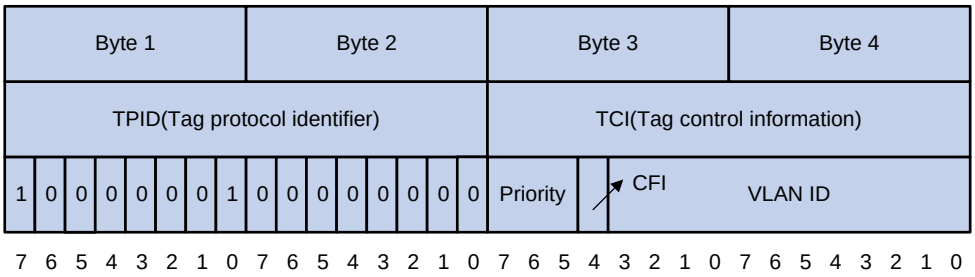


表1-2 802.1p 优先级说明

802.1p 优先级（十进制）	802.1p 优先级（二进制）	关键字
0	000	best-effort
1	001	background
2	010	spare
3	011	excellent-effort
4	100	controlled-load
5	101	video
6	110	voice

802.1p 优先级（十进制）	802.1p 优先级（二进制）	关键字
7	111	network-management

1.1.7 队列调度

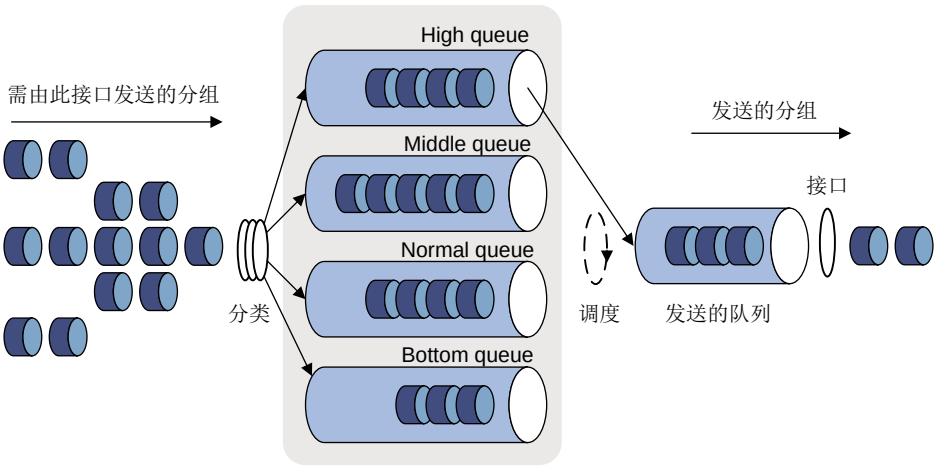
对于拥塞管理，一般采用队列技术，使用一个队列算法对流量进行分类，之后用某种优先级别算法将这些流量发送出去。每种队列算法都是用以解决特定的网络流量问题，并对带宽资源的分配、延迟、抖动等有着十分重要的影响。

这里介绍两种常用的硬件实现拥塞管理的队列调度机制：SP（Strict Priority，严格优先级）队列和WRR（Weighted Round Robin，加权轮询）队列。

1. SP 队列

SP 队列包含多个队列，分别对应不同的优先级，按优先级递减的顺序进行调度。SP 队列调度算法是针对关键业务型应用设计的。关键业务有一个重要的特点，即在拥塞发生时要求优先获得服务以减小响应的延迟。

图1-6 SP 队列示意图



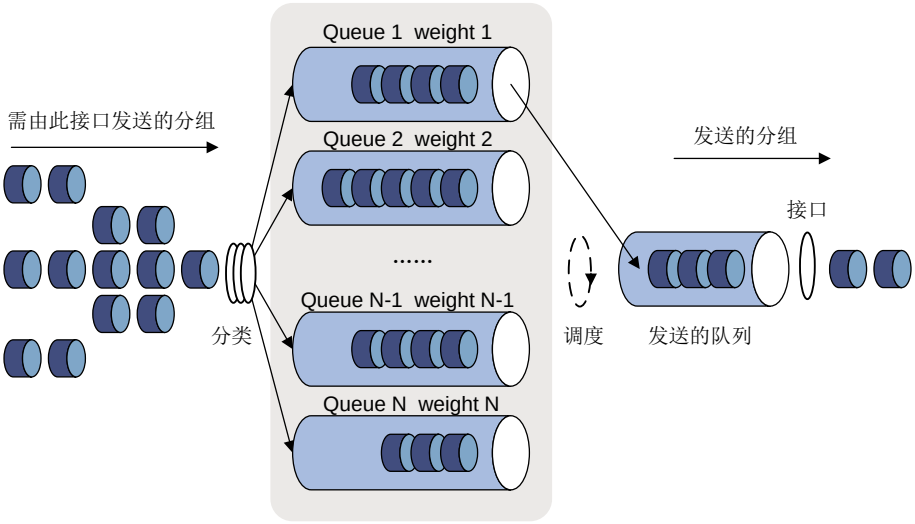
以端口有 8 个输出队列为例，优先队列将端口的 8 个输出队列分成 8 类，依次为 7、6、5、4、3、2、1、0 队列，它们的优先级依次降低。在队列调度时，SP 严格按照优先级从高到低的顺序优先发送较高优先级队列中的分组，当较高优先级队列为空时，再发送较低优先级队列中的分组。这样，将关键业务的分组放入较高优先级的队列，将非关键业务（如 E-Mail）的分组放入较低优先级的队列，可以保证关键业务的分组被优先传送，非关键业务的分组在处理关键业务数据的空闲间隙被传送。

SP 的缺点是如果较高优先级队列中长时间有分组存在，那么低优先级队列中的报文将一直得不到服务。

2. WRR 队列

WRR 队列调度算法在队列之间进行轮流调度，保证每个队列都得到一定的服务时间。

图1-7 WRR 队列示意图



以端口有 8 个输出队列为例，WRR 可为每个队列配置一个加权值（依次为 w7、w6、w5、w4、w3、w2、w1、w0），加权值表示获取资源的比重。如一个 100M 的端口，配置它的 WRR 队列调度算法的加权值为 25：25：15：15：5：5：5：5（依次对应 w7、w6、w5、w4、w3、w2、w1、w0），这样可以保证最低优先级队列至少获得 5Mbit/s 带宽，避免了采用 SP 调度时低优先级队列中的报文可能长时间得不到服务的缺点。WRR 队列还有一个优点是，虽然多个队列的调度是轮询进行的，但对每个队列不是固定地分配服务时间片——如果某个队列为空，那么马上换到下一个队列调度，这样带宽资源可以得到充分的利用。

基本 WRR 队列包含多个队列，用户可以定制各个队列的权重、百分比或字节计数，WRR 按用户设定的参数进行加权轮询调度。

说明

还可通过配置实现 SP+WRR 功能，即在配置 WRR 队列时，将某个或某些队列划分到 SP 组。此时，系统首先按照严格优先级对 SP 组中的队列进行调度。当 SP 组中的队列没有报文发送时，再按照 WRR 算法对其它队列进行调度。

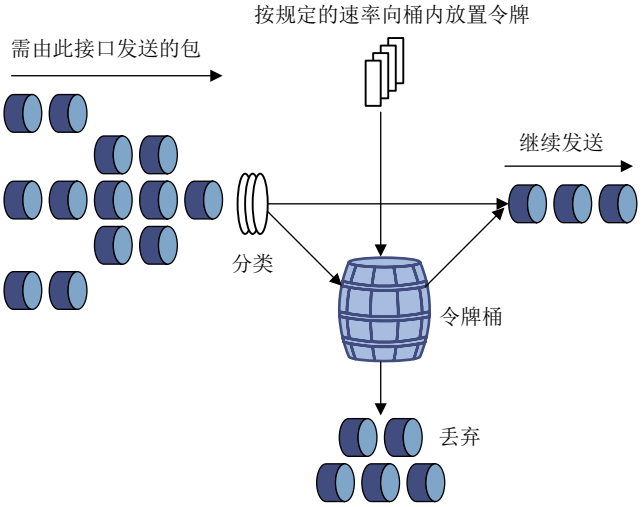
1.1.8 端口限速

端口限速是采用令牌桶进行流量控制的一种方法。利用端口限速可以在一个物理端口上限制发送报文（包括紧急报文）的总速率。端口限速能够限制在物理端口上通过的所有报文。

1. 令牌桶与流量评估

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。

图1-8 用令牌桶评估流量



在用令牌桶评估流量规格时，是以令牌桶中的令牌数量是否足够满足报文的转发为依据的。如果桶中存在足够的令牌可以用来转发报文（通常用一个令牌关联一个比特的转发权限），称流量遵守或符合（conforming）这个规格，否则称为不符合或超标（excess）。

评估流量时令牌桶的参数设置包括：

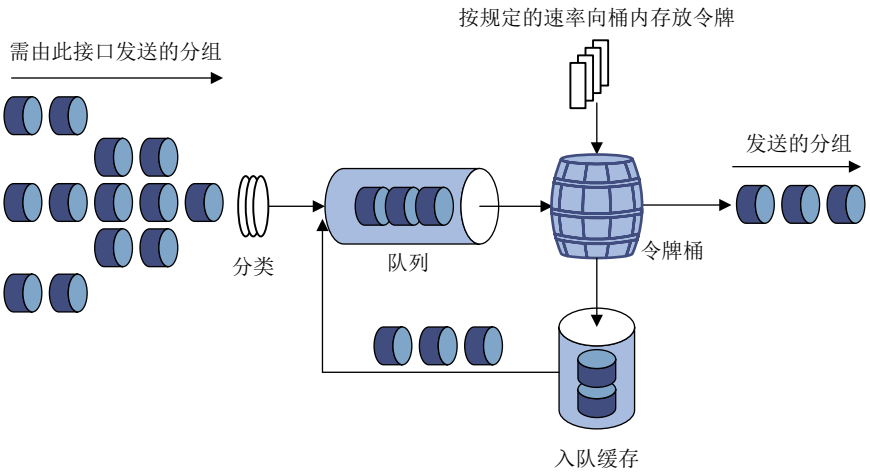
- 平均速率：向桶中放置令牌的速率，即允许的流的平均速度。通常设置为 CIR（Committed Information Rate，承诺信息速率）。
- 突发尺寸：令牌桶的容量，即每次突发所允许的最大的流量尺寸。通常设置为 CBS（Committed Burst Size，承诺突发尺寸），设置的突发尺寸必须大于最大报文长度。

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

2. 端口限速的工作机制

当设备的某个端口上配置了端口限速时，所有经由该端口发送的报文首先要经过端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，报文将进入 QoS 队列进行拥塞管理。这样，就可以对通过该物理端口的报文流量进行控制。

图1-9 端口限速处理过程示意图



由于采用了令牌桶控制流量，当令牌桶中存有令牌时，可以允许报文的突发性传输；当令牌桶中没有令牌时，报文必须等到桶中生成了新的令牌后才可以继续发送。这就限制了报文的流量不能大于令牌生成的速度，达到了限制流量，同时允许突发流量通过的目的。

1.1.9 优先级映射

1. 基本概念

在网络的入口需要为网络的流量打上一定的区分标记，这种标记用以标识流量的调度权重或者转发处理优先级别的高低。网络中间节点处理报文时，就可以根据报文的优先级来进行相应的调度。

报文在进入设备以后，设备会根据自身支持的情况和相应的规则给报文分配包括 802.1p 优先级、DSCP、本地优先级等在内的一系列参数。

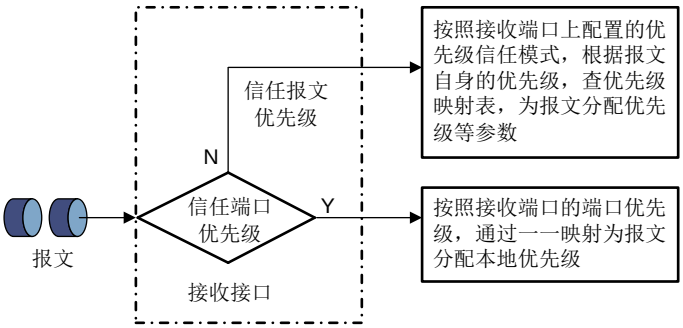
- 802.1p 优先级和 DSCP 优先级的介绍请参见 1.1.6 报文优先级。
- 本地优先级是指设备为报文分配的一种具有本地意义的优先级，对应出端口队列序号。本地优先级值越大的报文越被优先处理。

设备提供了两种端口优先级信任模式：

- 信任报文的优先级：按照接收端口上配置的优先级信任模式，根据报文自身的优先级，查找优先级映射表，为报文分配优先级参数。
- 信任端口的优先级：按照接收端口的端口优先级，通过一一映射为报文分配本地优先级。

用户可以根据需要配置端口优先级信任模式。设备上报文的优先级映射过程如下图所示。

图1-10 支持端口优先级信任模式的情况下优先级映射过程示意图



2. 优先级映射表介绍

设备提供了多张优先级映射表，分别对应相应的优先级映射关系。各个优先级的映射表和缺省取值如下所示。

- CoS to Queue：802.1p 优先级到本地优先级映射表。
- DSCP to Queue：DSCP 到本地优先级映射表，仅对 IP 报文生效。

映射表缺省取值如下所示。

表1-3 CoS to Queue 缺省映射关系

映射输入索引（CoS）	映射优先级（Queue）
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

表1-4 DSCP to Queue 缺省映射关系

映射输入索引（DSCP）	映射优先级（Queue）
0～7	0
8～15	1
16～23	2
24～31	3
32～39	4
40～47	5
48～55	6

映射输入索引（DSCP）	映射优先级（Queue）
56～63	7

1.2 QoS配置

1.2.1 配置概述

1. 配置 QoS 策略

QoS 策略包含了三个要素：类、流行为、策略。用户可以通过 QoS 策略将指定的类和流行为绑定起来，方便的进行 QoS 配置。

(1) 类

类是用来识别流的。

类的要素包括：类的名称和类的规则。

用户可以定义一系列的规则，来对报文进行分类。同时用户可以指定规则之间的关系：and 和 or。

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

(2) 流行为

流行为用来定义针对报文所做的 QoS 动作。

流行为的要素包括：流行为的名称和流行为中定义的动作。

用户可以在一个流行为中定义多个动作。

(3) 策略

QoS 策略支持基于端口的应用，即 QoS 策略对端口接收的流量生效。一个策略只能在一个端口上得到应用。每个端口只能在入方向上应用一个策略。

QoS 策略配置的推荐步骤如下表所示。

表1-5 QoS 策略配置步骤

步骤	配置任务	说明
1	1.2.2 新建策略	必选 新建一个策略

2. 配置队列调度

队列调度配置的推荐步骤如下表所示。

表1-6 队列调度配置步骤

步骤	配置任务	说明
1	1.2.3 在端口上配置队列	可选 在指定端口上配置队列调度的方式 产品不同，端口上缺省的队列算法可能不同

3. 配置优先级映射表

优先级映射表配置的推荐步骤如下表所示。

表1-7 优先级映射表配置步骤

步骤	配置任务	说明
1	1.2.4 配置优先级映射表	可选 设置不同类型映射表中的映射输入和映射优先级的对应关系

4. 配置端口优先级

端口优先级配置的推荐步骤如下表所示。

表1-8 端口优先级配置步骤

步骤	配置任务	说明
1	1.2.5 配置端口的优先级和信任模式	必选

5. 配置端口限速

端口限速配置的推荐步骤如下表所示。

表1-9 端口限速配置步骤

步骤	配置任务	说明
1	1.2.6 在端口上配置端口限速	必选 设置限制物理端口接收或者发送数据的速率

1.2.2 新建策略

(1) 在导航栏中选择“QoS > QoS 策略”，默认进入“接口”页签的页面，如下图所示。

图1-11 接口

(2) 配置 QoS 策略，详细配置如下表所示。

(3) 单击  完成操作，进入如下图所示页面。

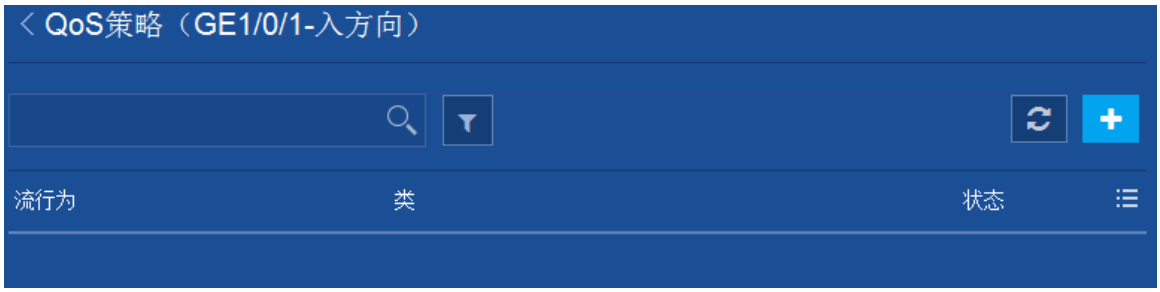
表1-10 QoS 策略的详细配置

配置项	说明
接口	设置要应用该QoS策略的接口，必须选择
入方向	设置应用QoS策略的方向： • 入方向：表示对端口接收到的报文应用 QoS 策略 • 出方向：表示对端口发送的报文应用 QoS 策略
出方向	

图1-12 QoS 策略

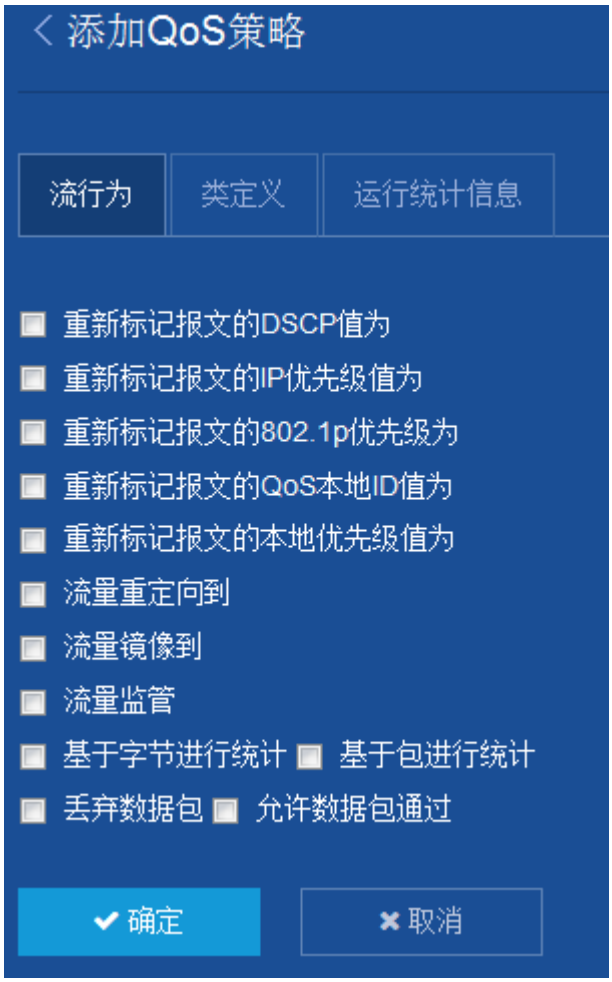
(4) 单击“策略详情”，进入下图所示的页面。（假设选择接口为 GE1/0/1，策略应用的方向为入方向。）

图1-13 QoS 策略（GE1/0/1-方向）



(5) 单击  ，默认进入“流行为”页签的页面，如下图所示。

图1-14 流行为



(6) 配置流行为的信息，详细配置如下表所示。

(7) 单击<确定>完成操作。

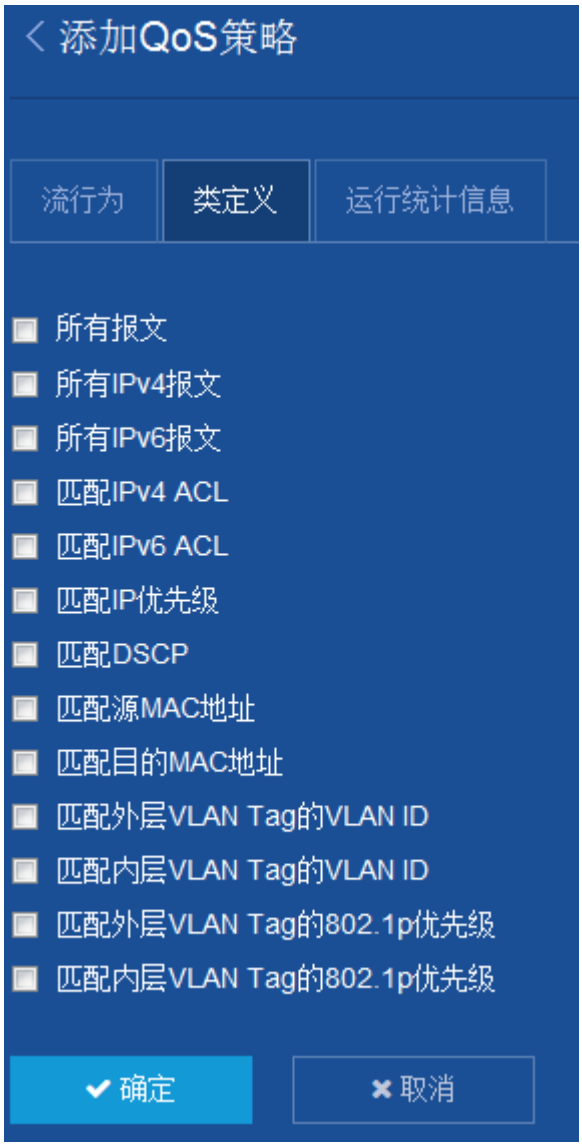
表1-11 流行为的详细配置

配置项	说明
重新标记报文的DSCP值为	重新设置标记报文的DSCP值
重新标记报文的IP优先级值为	重新设置标记报文的IP优先级值
重新标记报文的802.1p优先级为	重新设置标记报文的802.1p优先级
重新标记报文的QoS本地ID值为	重新设置标记报文的QoS本地ID值
重新标记报文的本地优先级值为	重新设置标记报文的本地优先级值
流量重定向到	流量重定向到CPU或指定接口

配置项	说明
流量镜像到	流量镜像到CPU或指定接口
流量监管	设置流量监管的措施，如下： • 承诺信息速率（CIR） • 承诺突发尺寸（CBS） • 超出突发尺寸（EBS） • 峰值速率（PIR） • 对绿色报文采取的动作 • 对黄色报文采取的动作 • 对红色报文采取的动作
基于字节进行统计	设置是否基于字节进行统计
基于包进行统计	设置是否基于包进行统计
丢弃数据包	设置是否丢弃数据包
允许数据包通过	设置是否允许数据包通过

(8) 单击“类定义”页签，进入如下图所示页面。

图1-15 类定义



(9) 配置类定义，详细配置如下表所示。

(10) 单击<确定>完成操作。

表1-12 类定义的详细配置

配置项	说明
所有报文	表示允许所有报文通过端口
所有IPv4报文	表示允许所有的IPv4报文通过端口
所有IPv6报文	表示允许所有的IPv6报文通过端口
匹配IPv4 ACL	设置匹配Ipv4 ACL的规则，依据IPv4 ACL规则识别出报文，仅该报文可以通过端口
匹配Ipv6 ACL	设置匹配Ipv6 ACL的规则，依据Ipv6 ACL规则识别出报文，仅该报文可以通过端口
匹配IP优先级	依据IP优先级识别出报文，仅该报文可以通过端口

配置项	说明
匹配DSCP	依据DSCP识别出报文，仅该报文可以通过端口
匹配源MAC地址	依据源MAC地址识别出报文，仅该报文可以通过端口
匹配目的MAC地址	依据目的MAC地址识别出报文，仅该报文可以通过端口
匹配外层VLAN Tag的VLAN ID	依据外层VLAN Tag的VLAN ID识别出报文，仅该报文可以通过端口
匹配内层VLAN Tag的VLAN ID	依据内层VLAN Tag的VLAN ID识别出报文，仅该报文可以通过端口
匹配外层VLAN Tag的802.1p优先级	依据外层VLAN Tag的802.1p优先级识别出报文，仅该报文可以通过端口
匹配内层VLAN Tag的802.1p优先级	依据内层VLAN Tag的802.1p优先级识别出报文，仅该报文可以通过端口

(11) 单击“运行统计信息”页签。

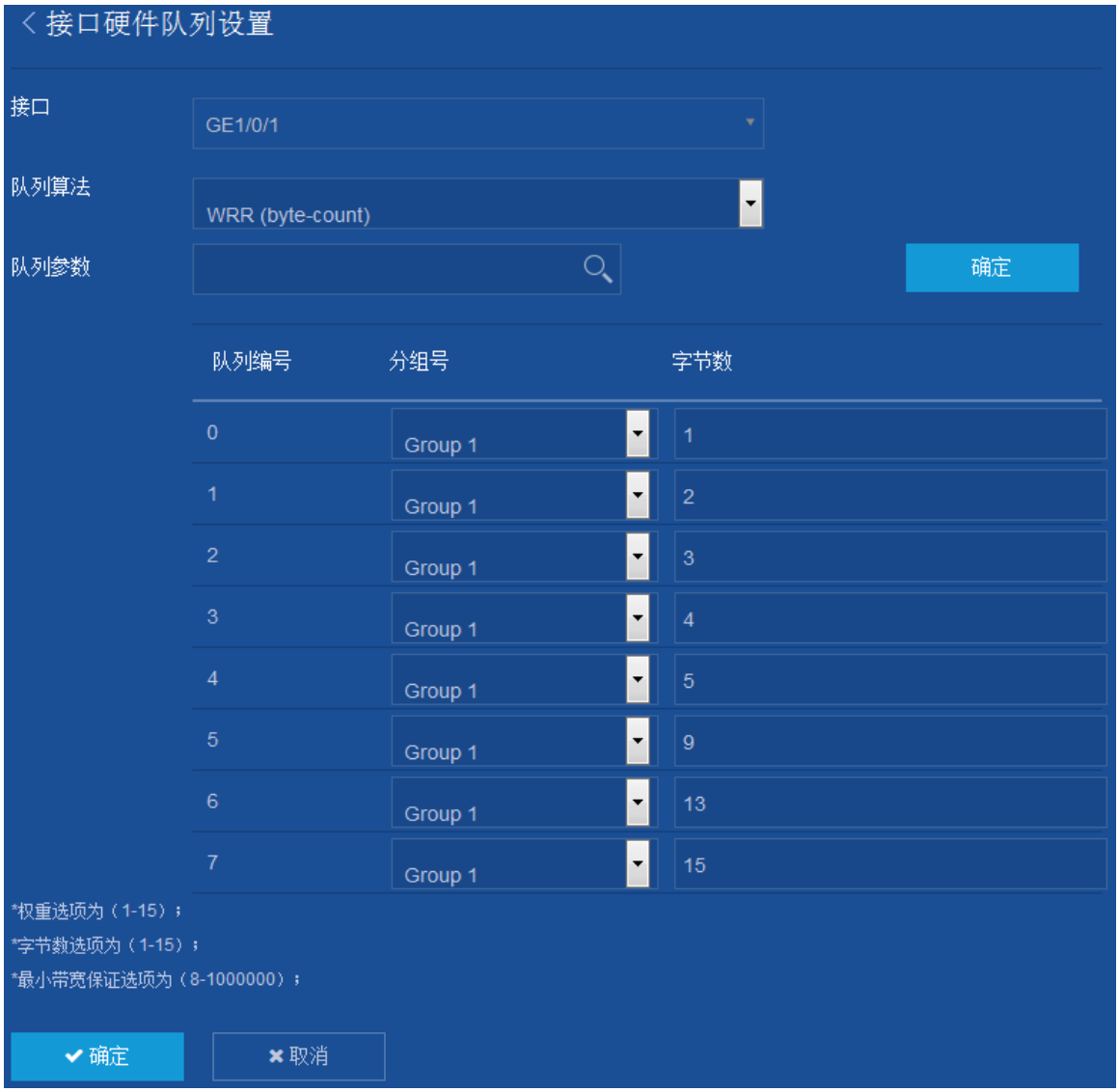
(12) 单击<确定>完成操作。

1.2.3 在端口上配置队列

(1) 在导航栏中选择“QoS > 硬件队列”。

(2) 单击需要设置的端口后的  ，进入硬件队列的配置页面，如下图所示。

图1-16 硬件队列



(3) 在端口上配置队列，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表1-13 在端口上配置队列的详细配置

配置项	说明
接口	显示需要配置队列的接口
队列算法	设置队列的算法，包括： • SP • WRR(weight) • WRR（byte-count） • WFQ(weight) • WFQ（byte-count）
队列编号	选择要配置的队列的编号 取值为0～7
分组号	设置该队列属于哪个优先组 队列序号选择某个值后可用，可选的优先组包括： • NA • Group SP：表示该队列属于严格优先组 • Group 1：表示该队列属于加权轮询队列优先组 1 • Group 2：表示该队列属于加权轮询队列优先组 2
权重	设置队列的调度权重 优先组为“1”时可用

1.2.4 配置优先级映射表

(1) 在导航栏中选择“QoS > 优先级映射”，默认进入“优先级映射表”页签的页面，如下图所示。

图1-17 优先级映射

(2) 配置优先级映射表，详细配置如下表所示。

(3) 单击<应用>按钮完成操作。

表1-14 优先级映射表的详细配置

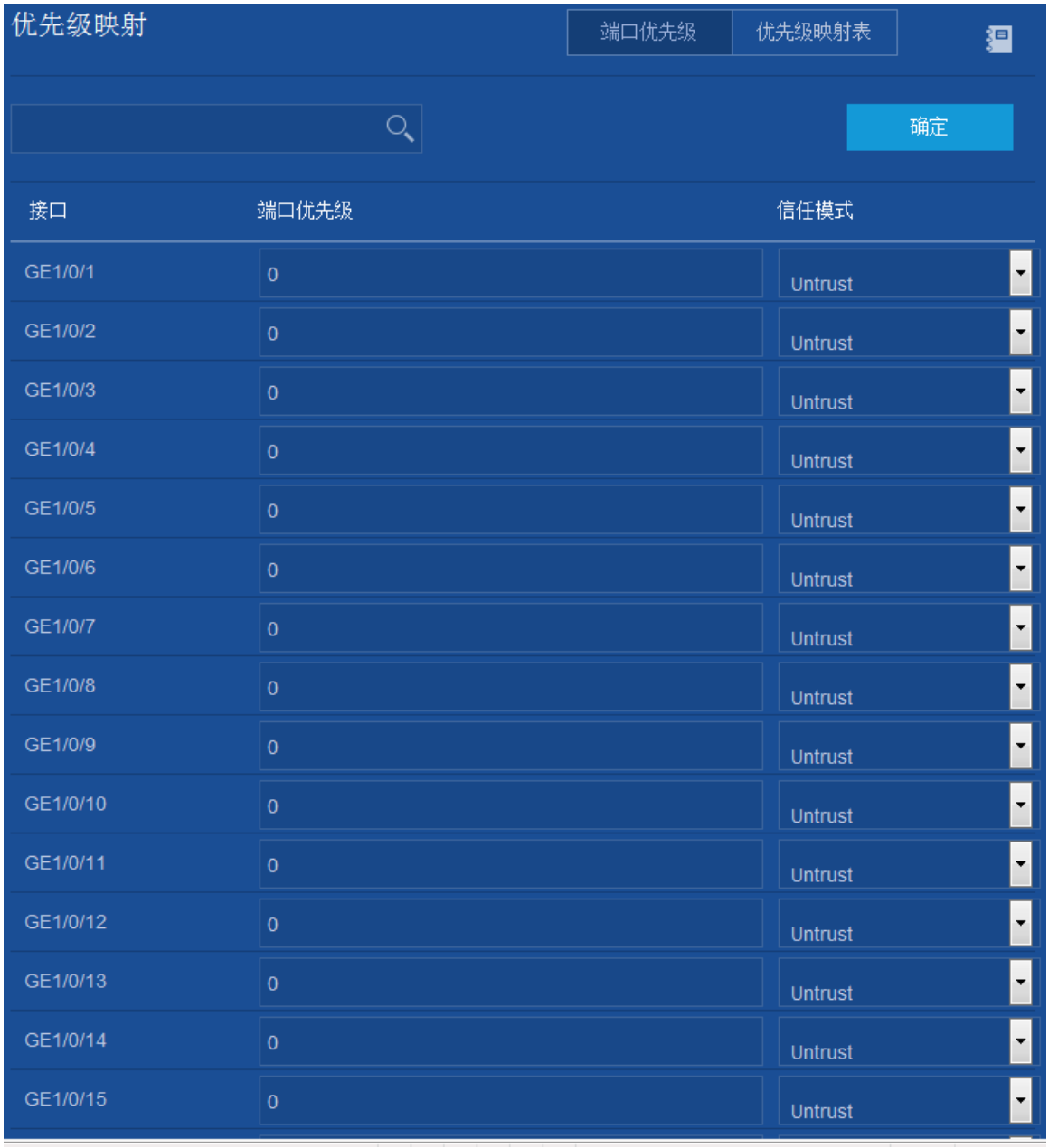
配置项	说明
映射表类型	设备要配置的映射表的类型，包括： • 802.1p 优先级到本地优先级映射表 • DSCP 到 802.1p 优先级映射表 • DSCP 到 DSCP 映射表
输入值	设置不同映射输入所对应的映射优先级的值
输出值	
<重置>	单击此按钮可以使当前映射表显示的映射优先级值都恢复到缺省的状态 需要注意的使，要恢复缺省配置，还必须要单击<应用>按钮才能生效

1.2.5 配置端口的优先级和信任模式

(1) 在导航栏中选择“QoS > 优先级映射”。

(2) 单击“端口优先级”页签，进入如下图所示的页面。

图1-18 端口优先级



(3) 配置端口优先级，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表1-15 端口优先级的详细配置

配置项	说明
接口	显示要配置的接口
端口优先级	设置端口本地优先级的值
信任模式	设置端口优先级信任模式： • Untrust：端口不信任报文的优先级 • 802.1p：信任报文自带的 802.1p 优先级，以此优先级进行优先级映射 • DSCP：信任 IP 报文自带的 DSCP 优先级，以此优先级进行优先级映射

1.2.6 在端口上配置端口限速

(1) 在导航栏中选择“QoS > 限速”。

(2) 单击，进入端口限速的配置页面，如下图所示。

图1-19 添加端口限速

(3) 配置端口限速，详细配置如下表所示。

(4) 单击<确定 >按钮完成操作。

表1-16 端口限速的详细配置

配置项	说明
接口	设置要配置端口限速的接口

配置项	说明
方向	设置对指定端口上哪个方向的数据流进行限速 • 入方向：表示对指定端口接收到的数据流进行限速 • 出方向：表示对指定端口发送的数据流进行限速
承诺信息速率（CIR）	设置承诺信息速率，流量的平均速率
承诺突发尺寸（CBS）	设置承诺突发尺寸，每个时间间隔可发送的字节数

1.3 注意事项

当 ACL 作为 QoS 策略中流分类的匹配条件时，ACL 仅用于匹配报文，ACL 规则中的动作（**deny** 或 **permit**）被忽略，不作为对报文进行丢弃或转发的依据。

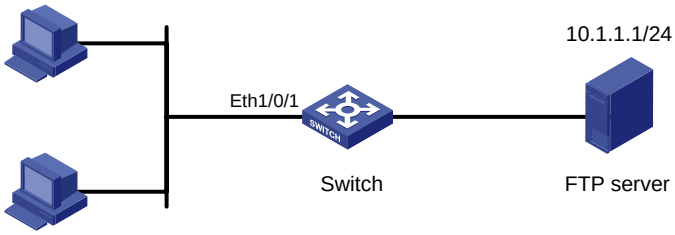
2 ACL/QoS 典型配置举例

2.1 ACL/QoS配置举例

1. 组网需求

- 如下图所示，Switch 与 FTP 服务器（IP 地址为 10.1.1.1/24）相连，用户通过 Ethernet1/0/1 接入 Switch。
- 要求正确配置 ACL 和 QoS 策略，禁止用户在每天的 8:00～18:00 访问 FTP 服务器。

图2-1 ACL/QoS 配置组网图



2. 配置思路

采用如下思路进行配置：

(1) 配置限制用户在每天的 8:00～18:00 访问 FTP 服务器的 ACL 规则。

(2) 配置 QoS 策略为：匹配该 ACL 规则的类，采取丢弃数据包的动作。

(3) 在 Ethernet1/0/1 的入方向上应用该 QoS 策略。

3. 配置步骤

(1) 定义每天 8:00 至 18:00 的周期时间段。

步骤 1：在导航栏中选择“资源 > 时间段”。

步骤 2：单击。

步骤 3：进行如下配置，如下图所示。

- 输入名称为“test-time”。
- 设置开始时间为“8:00”，结束时间为“18:00”。
- 选中“周日”～“周六”前的复选框。

步骤 4：单击<确定>按钮完成操作。

图2-2 定义每天 8:00 至 18:00 的周期时间段

(2) 新建高级 IPv4 ACL。

步骤 1：在导航栏中选择“资源 > IPv4”。

步骤 2：单击  。

步骤 3：进行如下配置，如下图所示。

- 设置类型为“高级 ACL”。
- 设置编号为“3000”。
- 选择“开始添加规则”前的复选框。

步骤 4：单击<确定>按钮完成操作。

图2-3 新建高级 IPv4 ACL

(3) 配置到 FTP 服务器的访问规则。

步骤 1：单击“高级配置”页签。

步骤 2：进行如下配置，如下图所示。

- 输入规则编号为“2”。
- 选择动作为“允许”。
- 选择 IP 协议类型为 IP，即“256”。
- 选中“匹配目的 IP 地址/通配符掩码”前的复选框，输入目的 IP 地址为“10.1.1.1”，输入目的地址通配符为“0.0.0.0”。
- 选择时间段为“test-time”。

步骤 3：单击<确定>按钮完成操作。

图2-4 配置到 FTP 服务器的访问规则

(4) 新建策略。

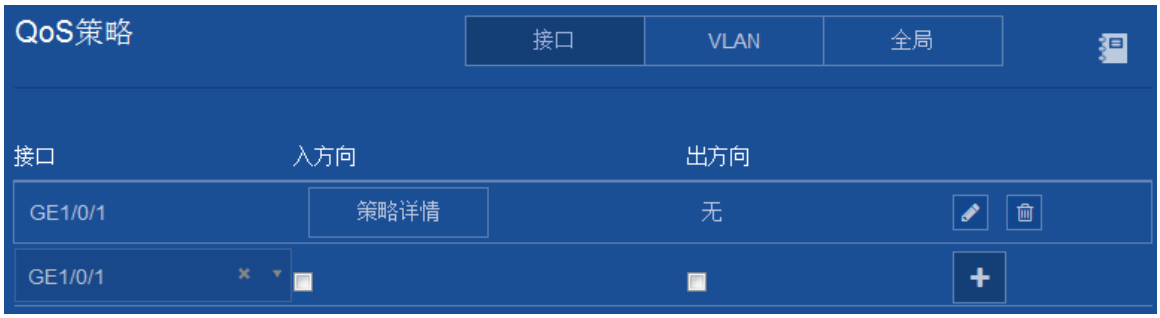
步骤 1：在导航栏中选择“QoS > QoS 策略”。

步骤 2：进行如下配置，如下图所示。

- 设置接口为“GE1/0/1”。
- 选择“入方向”下的复选框。

步骤 3：单击  完成操作，进入如下图所示页面。

图2-5 QoS 策略



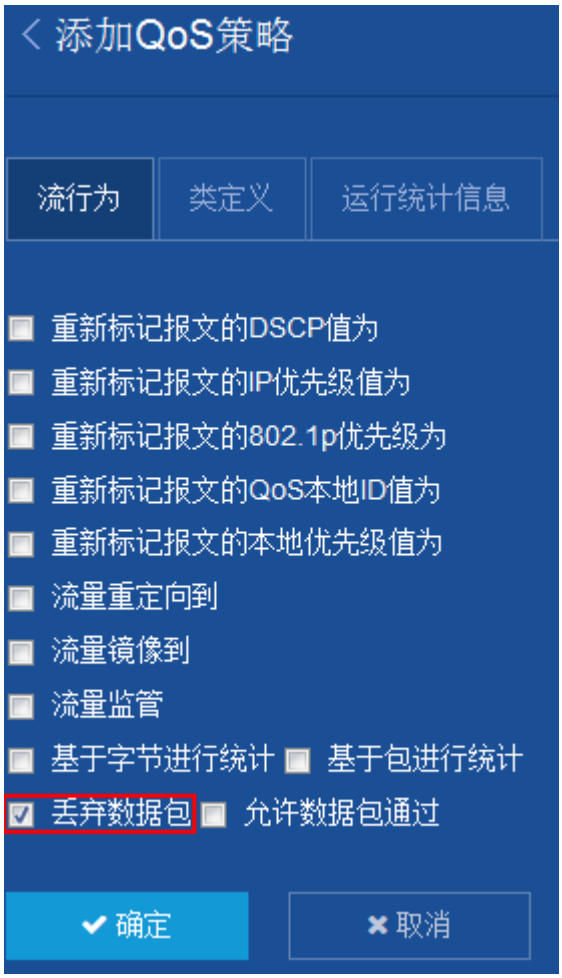
步骤 4：单击“策略详情”。

步骤 5：单击  。

步骤 6：进行如下配置，如下图所示。

- 选择“丢弃数据包”前的复选框。

图2-6 流行为



步骤 7：单击“类定义”页签.

步骤 8：进行如下配置，如下图所示。

- 选择“匹配 IPv4 ACL”前的复选框。
- 选择 IPv4 ACL 为“3000”。

图2-7 类定义

步骤 9：单击“运行统计信息”页签。

步骤 10：单击<确定>完成操作，状态显示为“成功”，如下图所示。

图2-8 配置策略成功