

目 录

第 1 章 QoS 简介.....	1-1
1.1 概述.....	1-1
1.2 传统的分组投递业务.....	1-1
1.3 新业务引发的新需求.....	1-1
1.4 拥塞的产生、影响和对策.....	1-2
1.4.1 拥塞的产生	1-2
1.4.2 拥塞的影响	1-2
1.4.3 对策.....	1-3
1.5 几种主要的流量管理技术.....	1-3
第 2 章 流分类、流量监管和流量整形.....	2-1
2.1 流分类简介	2-1
2.2 流量监管和流量整形简介.....	2-1
2.2.1 流量评估与令牌桶.....	2-2
2.2.2 流量监管.....	2-3
2.2.3 流量整形.....	2-3
2.2.4 物理接口限速.....	2-4
2.3 流量监管和流量整形配置.....	2-5
2.3.1 流量监管配置.....	2-5
2.3.2 流量整形配置.....	2-7
2.3.3 接口限速配置.....	2-7
2.4 流量监管与流量整形显示和调试	2-7
2.4.1 显示 TP 规则.....	2-7
2.4.2 显示 TP 在各接口上信息	2-8
2.4.3 显示接口的 TS 配置情况和统计信息.....	2-8
2.4.4 显示接口的 LR 配置情况和统计信息.....	2-8
2.5 流量监管与流量监控典型配置举例.....	2-9
第 3 章 拥塞管理	3-1
3.1 拥塞管理简介	3-1
3.1.1 拥塞管理策略.....	3-1
3.1.2 拥塞管理技术的对比	3-5
3.2 先进先出队列的配置.....	3-6
3.2.1 配置 FIFO 队列的长度.....	3-7
3.3 优先队列的配置.....	3-7
3.3.1 配置优先列表.....	3-7
3.3.2 在接口上应用优先列表组.....	3-9

3.3.3 优先队列的显示和调试.....	3-9
3.4 定制队列的配置.....	3-10
3.4.1 配置定制列表.....	3-10
3.4.2 在接口上应用定制列表.....	3-12
3.4.3 定制队列的显示和调试.....	3-12
3.5 加权公平队列的配置.....	3-12
3.5.1 在接口上应用加权公平队列.....	3-13
3.5.2 加权公平队列的显示和调试.....	3-13
3.6 基于类的队列的配置.....	3-13
3.6.1 配置接口最大可用带宽.....	3-14
3.6.2 定义类并配置其匹配规则.....	3-15
3.6.3 定义流行为并配置其特性.....	3-18
3.6.4 配置策略.....	3-25
3.6.5 应用策略.....	3-26
3.6.6 基于类的队列的显示和调试.....	3-27
3.7 RTP 优先队列的配置.....	3-28
3.7.1 在接口上应用 RTP 队列.....	3-28
3.7.2 配置最大预留带宽.....	3-28
3.7.3 RTP 报文队列的显示和调试.....	3-29
3.7.4 QoS 令牌功能.....	3-29
3.8 典型配置举例.....	3-30
3.8.1 优先队列配置举例.....	3-30
3.8.2 基于类的队列配置举例.....	3-31
3.8.3 定制队列配置举例.....	3-32
3.8.4 CBQ 基于类的队列配置举例.....	3-34
3.8.5 Qos 策略嵌套及 LR 综合应用配置举例.....	3-36
3.8.6 ATM PVC Remark 策略典型配置举例.....	3-37
第 4 章 拥塞避免.....	4-1
4.1 拥塞避免简介.....	4-1
4.2 WRED 的配置.....	4-2
4.2.1 使用 WRED.....	4-2
4.2.2 设置 WRED 计算平均队列长度的指数.....	4-3
4.2.3 设置 WRED 各优先级参数.....	4-3
4.3 WRED 的显示和调试.....	4-4
第 5 章 帧中继 QoS.....	5-1
5.1 帧中继 QoS 简介.....	5-1
5.1.1 帧中继 QoS.....	5-1
5.1.2 重要参数.....	5-1
5.1.3 帧中继 OoS 的实现.....	5-2
5.2 帧中继 OoS 的配置.....	5-7

5.2.1 创建和配置帧中继 class	5-7
5.2.2 配置帧中继流量整形	5-9
5.2.3 配置帧中继流量监管	5-10
5.2.4 配置帧中继拥塞管理	5-11
5.2.5 配置帧中继 DE 规则列表	5-12
5.2.6 配置帧中继队列管理	5-13
5.2.7 配置帧中继分片	5-15
5.3 帧中继 QoS 的显示和调试	5-16
5.4 帧中继 QoS 典型配置举例	5-16
5.4.1 帧中继流量整形配置举例	5-16
5.4.2 帧中继分片配置举例	5-17
第 6 章 MPLS QoS	6-1
6.1 MPLS QoS 概述	6-1
6.2 MPLS QoS 配置	6-1
6.2.1 配置 MPLS PQ	6-1
6.2.2 配置 MPLS CQ	6-2
6.2.3 配置 MPLS CBQ	6-3
6.2.4 配置 MPLS CAR	6-5
6.3 MPLS QoS 典型配置举例	6-6
6.3.1 对同一 VPN 内的流进行 QoS 配置	6-6

第1章 QoS 简介

1.1 概述

服务质量 (Quality of Service, 简称 QoS) 是各种存在服务供需关系的场合中普遍存在的概念, 它评估服务方满足客户服务需求的能力。评估通常不是精确的评分, 而是注重分析在什么条件下服务是好的, 在什么情况下还存在着不足, 以便有针对性地作出改进。

在因特网中, QoS 所评估的就是网络投递分组的服务能力。由于网络提供的服务是多样的, 因此对 QoS 的评估可以基于不同方面。通常所说的 QoS, 是对分组投递过程中可为延迟、延迟抖动、丢包率等核心需求提供支持的服务能力的评估。

1.2 传统的分组投递业务

传统的 IP 网络无区别地对待所有的报文, 路由器处理报文采用的策略是先进先出 FIFO (First In First Out), 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路由器的资源, 至于得到资源的多少完全取决于报文到达的时机。这种服务策略称作 Best-Effort (尽力而为), 它尽最大的努力将报文送到目的地, 但对分组投递的延迟、延迟抖动、丢包率和可靠性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、延迟性能不敏感的 WWW、文件传输、e-mail 等业务。

1.3 新业务引发的新需求

随着计算机网络的高速发展, 越来越多的网络接入因特网。Internet 无论从规模、覆盖范围和用户数量上都拓展得非常快。越来越多的用户使用 Internet 作为数据传输的平台, 开展各种应用。同样地, 服务提供商也希望通过新业务的开展来增加收益。

除了传统的 WWW、e-mail、FTP 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、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、低延迟和低延迟抖动的保证。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，而是还希望在投递过程中得到更好的服务，诸如支持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、设置报文的优先级。所有这些，都要求网络应当具备更为完善的服务能力。

1.4 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服务速率下降（引入了额外的延迟）的一种现象。

1.4.1 拥塞的产生

在因特网分组交换的复杂环境下，拥塞极为常见。以下图中的两种情况为例：

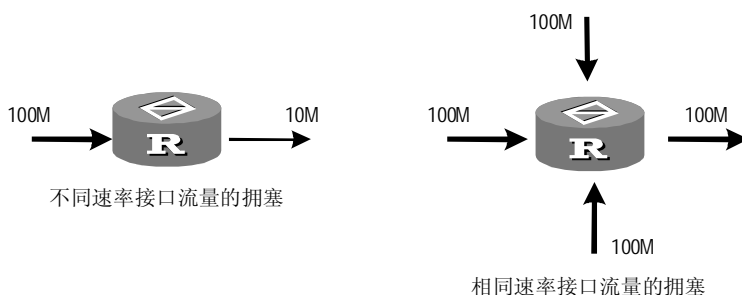


图1-1 流量拥塞示意图

- (1) 分组流从高速链路进入路由器，由低速链路转发出去。
- (2) 分组流从相同速率的多个接口同时进入路由器，由一个相同速率的接口转发出去。

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，任何用以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。

1.4.2 拥塞的影响

拥塞有可能会引发一系列的负面影响：

- l 拥塞增加了报文传输的延迟和延迟抖动。
- l 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，造成网络资源的损害。
- | 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。然而在分组交换以及多用户业务并存的复杂环境下，拥塞又是常见的，因此必须慎重加以对待。

1.4.3 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增加网络层在流量控制和资源分配上的功能，为有不同服务需求的业务提供有区别的服务，正确地分配和使用资源。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间接因素，减少拥塞发生的概率；并在拥塞发生时，依据业务的性质及其需求特性权衡资源的分配，将拥塞对 QoS 的影响减到最小。

1.5 几种主要的流量管理技术

流分类、流量监管、流量整形、拥塞管理、拥塞避免和物理接口限速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对象。流分类是有区别地实施服务的前提。
- | 流量监管：对进入路由器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，以保护运营商的商业利益和网络资源不受损害。流量监管是在 IP 层上实现的。
- | 拥塞管理：网络拥塞是必须采取的解决资源竞争的措施。通常是将报文放入队列中缓存，并采取某种调度算法安排报文的转发次序。
- | 拥塞避免：过度的拥塞会对网络资源造成损害。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。
- | 流量整形：一种主动调整流的输出速率的流控措施，通常是为了使流量适配下游路由器可供的网络资源，避免不必要的报文丢弃和拥塞。流量整形也是在 IP 层上实现的。
- | 物理接口限速：与 TP 相比，LR 能够限制在物理接口上通过的所有报文。TP 在 IP 层实现，对于不经过 IP 层处理的报文不起作用。当用户只要求对所有报文限速时，使用 LR 比较简单。

在这些流量管理技术中，流分类是基础，它依据一定的匹配规则识别出报文，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。

一般情况下，QoS 执行以下功能：

- | 流分类
- | 流量监管和流量整形
- | 拥塞管理
- | 拥塞避免

第2章 流分类、流量监管和流量整形

2.1 流分类简介

流分类采用一定的规则识别符合某类特征的报文，它是有区别地进行服务的前提和基础。

流分类规则可以使用 IP 报文头的 ToS 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。一般的分类依据都局限在封装报文的头部信息，使用报文的内容作为分类的标准是比较少见的。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、协议号码、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。而队列技术如 WFQ 也可以使用这个优先级来对报文进行不同的处理。下游（downstream）网络可以选择接收上游（upstream）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；流出结点之前进行整形；拥塞时的队列调度管理；拥塞加剧时要采取拥塞避免措施等。

2.2 流量监管和流量整形简介

如果不限用户发送的流量，那么大量用户不断突发的数据只会使网络更拥挤。为了使有限的网络资源能够更好地发挥效用，更好地为更多的用户服务，必须对用户的流量加以限制。比如限制每个时间间隔某个流只能得到承诺分配给它的那部分资源，防止由于过分突发所引发的网络拥塞。

流量监管和流量整形就是一种通过对流量规格的监督，来限制流量及其资源使用的流控策略。进行流量监管或整形有一个前提条件，就是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策略。一般采用令牌桶（Token Bucket）对流量的规格进行评估。

2.2.1 流量评估与令牌桶

1. 令牌桶的特点

令牌桶可以看是一个存放令牌的容器，它有一定的容量。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。

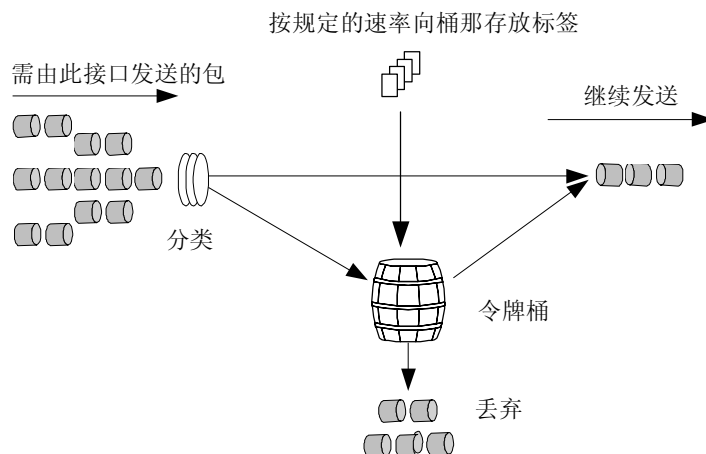


图2-1 用令牌桶评测流量

2. 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（conform）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：

- 1 平均速率：向桶中放置令牌的速率，即允许的流的平均速度。通常设置为承诺信息速率（Committed Information Rate，CIR）。
- 1 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。通常设置为承诺突发尺寸（Committed Burst Size，CBS），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。

3. 复杂评估

为了评估更复杂的情况，实施更灵活的调控策略，可以设置两个令牌桶。例如流量策略（Traffic Policing，简称 TP）中有三个参数：

- 1 承诺信息速率 CIR（Committed Information Rate）

- | 承诺突发尺寸 CBS (Committed Burst Size)
- | 超出突发尺寸 EBS (Excess Burst Size)

它使用了两个令牌桶，每个桶投放令牌的速率一样，均为 CIR，只是尺寸不同——分别为 CBS 和 CBS+EBS（这两个桶简称 C 桶和 E 桶），代表所允许的不同突发级别。每次评估时，依据“C 桶有足够的令牌”、“C 桶令牌不足，但 E 桶足够”以及“C 桶和 E 桶都没有足够的令牌”的情况，可以分别实施不同的流控策略。

2.2.2 流量监管

流量监管 (Traffic Policing) 的典型应用是监督进入网络的某一流量的规格，把它限制在一个合理的范围之内，或对超出的部分流量进行“惩罚”，以保护网络资源和运营商的利益，例如可以限制 HTTP 报文不能占用超过 50% 的网络带宽。如果发现某个连接的流量超标，流量监管可以选择丢弃报文，或重新设置报文的优先级。

流量监管的一个实例是 TP (Traffic Policing, 流量策略)，它广泛地用于监管进入因特网服务提供商 ISP 的网络流量。TP 还包括对所监管流量的流分类服务，并依据不同的评估结果，实施预先设定好的监管动作。这些动作可以是：

- | 转发：比如对评估结果为“符合”的报文继续正常转发的处理，也可以为 Diff-Serv 提供代为标记 DSCP 的服务再转发。
- | 丢弃：比如对评估结果为“不符合”的报文进行丢弃。
- | 改变优先级并转发：比如对评估结果为“部分符合”的报文，将之标记为其它的优先级后再进行转发。
- | 进入下一级的监管：流量监管可以逐级堆叠，每级关注和监管更具体的目标。

2.2.3 流量整形

流量整形 (Traffic Shaping) 是一种主动调整流量输出速率的措施。一个典型应用是基于下游网络结点的 TP 指标来控制本地流量的输出。

流量整形与流量监管的主要区别在于，流量整形对流量监管中需要丢弃的报文进行缓存——通常是它们放入缓冲区或队列内，也称流量整形 (Traffic Shaping, 简称 TS)，如图 2-2 所示。当令牌桶有足够的令牌时，再均匀的向外发送这些被缓存的报文。流量大小稳定在 CIR 速率的附近，其波动的幅度由预先设定的 CBS 值决定。流量整形与流量监管的另一区别是，整形可能会增加延迟，而监管几乎不引入额外的延迟。

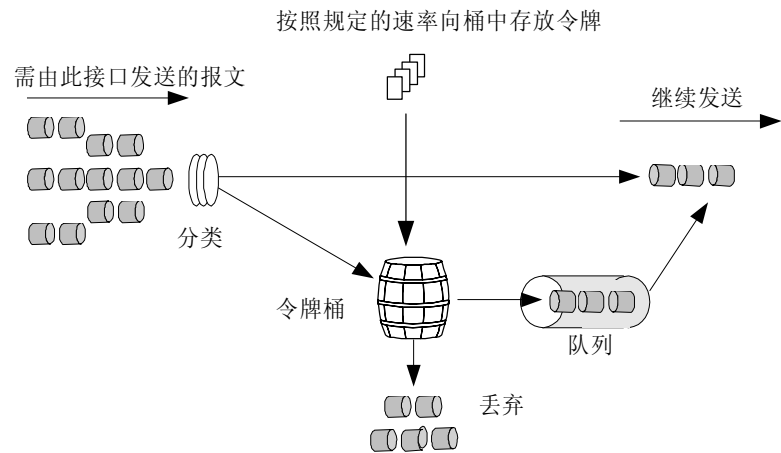


图2-2 TS 示意图

例如，在下图所示的应用中，路由器 RouterA 向 RouterB 发送报文。RouterB 要对 RouterA 发送来的报文进行 TP 监管，对超出规格的流量直接丢弃。

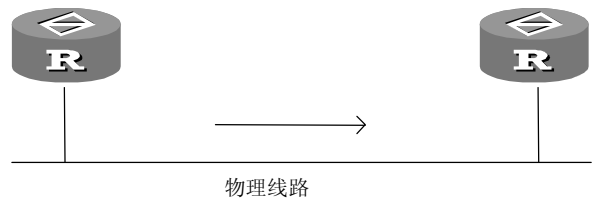


图2-3 流量整形的应用

为了减少报文的无谓丢失，可以在 RouterA 的出口对报文进行 TS 处理。将超出 TS 流量特性的报文缓存在 RouterA 中。当可以继续发送下一批报文时，TS 再从缓冲队列中取出报文进行发送。这样，发向 RouterB 的报文将都符合 RouterB 的流量规定。

2.2.4 物理接口限速

利用物理接口限速（Line Rate, LR）可以在一个物理接口上限制发送报文（包括紧急报文）的总速率。

LR 也是采用令牌桶进行流量控制。如果在路由器的某个接口上配置了 LR，所有经由该接口发送的报文首先要经过 LR 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，报文将入 QoS 队列进行拥塞管理。这样，就可以对通过该物理接口的报文流量进行控制。

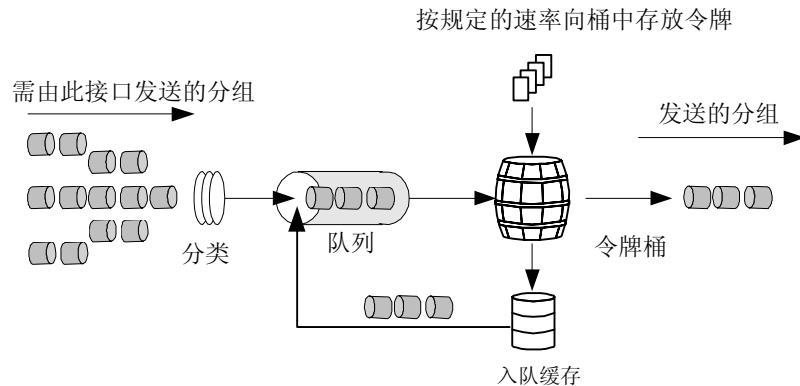


图2-4 LR 处理过程示意图

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。

与 TP 相比，LR 能够限制在物理接口上通过的所有报文。TP 在 IP 层实现，对于不经过 IP 层处理的报文不起作用。当用户只要求对所有报文限速时，使用 LR 比较简单。

2.3 流量监管和流量整形配置

流量监管配置主要包括：

- | 配置 TP 列表
- | 应用 TP 策略

流量整形配置主要包括：

- | 为某一类别的流设置整形参数
- | 为所有的流设置整形参数

物理接口限速配置主要包括：

- | 设置物理接口限速 LR

2.3.1 流量监管配置

流量监管的配置包括两方面的任务，一是定义那些需要实施监管的报文的特征，二是定义对这些报文的监管策略。

1. 配置 TP 列表

对于不同的 *carl-index*，本命令的重复执行将创建多个 TP 列表；对于同一个 *carl-index*，本命令的重复执行将修改 TP 列表的参数。

请在系统视图下进行下列配置。

表2-1 配置 TP 列表

操作	命令
创建/修改 TP 列表	qos carl <i>carl-index</i> { precedence <i>precedence-value</i> mac <i>mac-address</i> }
删除 TP 列表	undo qos carl <i>carl-index</i>

当需要在一条 TP 列表中同时匹配多个优先级时，可指定多个不同的 *precedence-value*。

2. 应用 TP 策略

本命令的重复执行将在接口上配置多个 TP 策略。本命令只对 IP 数据包进行处理，对其他的数据包不进行处理。

请在接口视图下进行下列配置。

表2-2 应用 TP 策略

操作	命令
应用 TP 策略	qos car { inbound outbound } { any acl <i>acl-number</i> carl <i>carl-index</i> } cir <i>committed-information-rate</i> cbs <i>committed-burst-size</i> ebs <i>excess-burst-size</i> green <i>action</i> red <i>action</i>
删除 TP 策略	undo qos car { inbound outbound } { any acl <i>acl-number</i> carl <i>carl-index</i> } cir <i>committed-information-rate</i> cbs <i>committed-burst-size</i> ebs <i>excess-burst-size</i>

命令中对数据包采取的动作 (*action*) 有以下几种：

- l **continue**: 继续由下一个 CAR 策略处理。
- l **discard**: 丢弃数据包。
- l **pass**: 发送数据包。
- l **remark-prec-continue** *new-precedence* : 设置新的 IP 优先级 *new-precedence*，并继续由下一个 CAR 策略处理，取值范围 0~7。
- l **remark-prec-pass** *new-precedence*: 设置新的 IP 优先级 *new-precedence*，并发送数据包到目的地址，取值范围 0~7。

TP 策略可以应用于报文到达的接口，也可应用于报文离开的接口。

2.3.2 流量整形配置

为某一类流或所有的流设置整形参数就可以使系统开始进行整形。

qos gts acl 用来为符合某一 ACL 的流设置整形参数，使用不同的 ACL 可以为不同的流设置整形参数。

qos gts any 用来为所有的流设置整形参数，重复使用将替代原来的设置。

qos gts acl 不能和 **qos gts any** 同时使用。

请在接口视图下进行下列设置。

表2-3 为某一类别的流或所有流设置整形参数

操作	命令
为某一类别的流设置整形参数	qos gts { any acl acl-number } cir committed-information-rate [cbs committed-burst-size [ebs excess-burst-size [queue-length queue-length]]]
取消对某一类别的流整形	undo qos gts { any acl acl-number }

2.3.3 接口限速配置

配置接口限速就是限制物理接口或 Tunnel 接口向外发送数据的速率。

Tunnel 接口限速结合各种队列调度算法可以实现 Tunnel 接口的拥塞管理。在为 Tunnel 接口配置队列之前，必须先在 Tunnel 接口上应用 LR。反之，在删除 Tunnel 接口上的 **qos lr** 命令时，必须先删除 Tunnel 接口上的队列配置。

请在接口（含 MFR 接口）视图下进行下列配置。

表2-4 设置接口限速

操作	命令
设置接口限速	qos lr cir committed-information-rate [cbs committed-burst-size [ebs excess-burst-size]]
取消接口限速	undo qos lr

2.4 流量监管与流量整形显示和调试

2.4.1 显示 TP 规则

在完成上述配置后，在所有视图下执行 **display** 命令可以显示 TP 的某条规则或所有访问规则，通过查看显示信息验证配置的效果。

表2-5 显示 TP 规则

操作	命令
显示 TP 规则	display qos carl [<i>carl-index</i>]

2.4.2 显示 TP 在各接口上信息

在完成上述配置后，在所有视图下执行 **display** 命令可以显示 TP 在各接口上的参数设置情况和运行统计信息，通过查看显示信息验证配置的效果。

表2-6 显示 TP 在各接口上信息

操作	命令
显示 TP 在各接口上信息	display qos car interface [<i>interface-type</i> <i>interface-number</i>]

2.4.3 显示接口的 TS 配置情况和统计信息

在完成上述配置后，在所有视图下执行 **display** 命令可以显示某个接口或所有接口的 TS 配置情况和统计信息，通过查看显示信息验证配置的效果。

表2-7 显示接口的 TS 配置情况和统计信息

操作	命令
显示接口的 TS 配置情况和统计信息	display qos gts interface [<i>interface-type</i> <i>interface-number</i>]

2.4.4 显示接口的 LR 配置情况和统计信息

在完成上述配置后，在所有视图下执行 **display** 命令可以显示某个接口或所有接口的 LR 配置情况和统计信息，通过查看显示信息验证配置的效果。

表2-8 显示接口的 LR 配置情况和统计信息

操作	命令
显示接口的 LR 配置情况和统计信息	display qos lr-interface [<i>interface-type</i> <i>interface-number</i>]

2.5 流量监管与流量监控典型配置举例

1. 配置需求

如图 2-5 所示，路由器 Quidway1 通过接口 ethernet0/0/0 和路由器 Quidway2 的接口 ethernet1/0/0 互连，Server、PC1、PC2 可经由 Quidway1 和 Quidway2 访问 Internet。Server、PC1 与 Quidway1 的 ethernet1/0/0 接口在同一网段，PC2 与 Quidway1 的 ethernet2/0/0 接口在同一网段。要求在路由器 Quidway2 上对接口 ethernet1/0/0 接收到的源自 Server 和 PC1 的报文流分别实施流量控制如下：

来自 server 的报文流量约束为 54000bps，流量小于 54000bps 时可以正常发送，流量超过 54000bps 时则将违规报文的优先级设置为 0 后进行发送；

来自 PC1 的报文流量约束为 80000bps，流量小于 80000bps 时可以正常发送，流量超过 80000bps 时则丢弃违规报文；

同时，对路由器 Quidway2 的 ethernet 1/0/0 和 ethernet 0/0/0 接口收发报文有如下要求：

- 1. Quidway2 的 ethernet 1/0/0 接口接收报文的总流量限制为 0.5Mbps，如果超过流量限制则将违规报文丢弃；
- 2. 经由 Quidway2 的 ethernet 0/0/0 接口进入 Internet 的报文流量限制为 1Mbps，如果超过流量限制则将违规报文丢弃。

2. 组网图

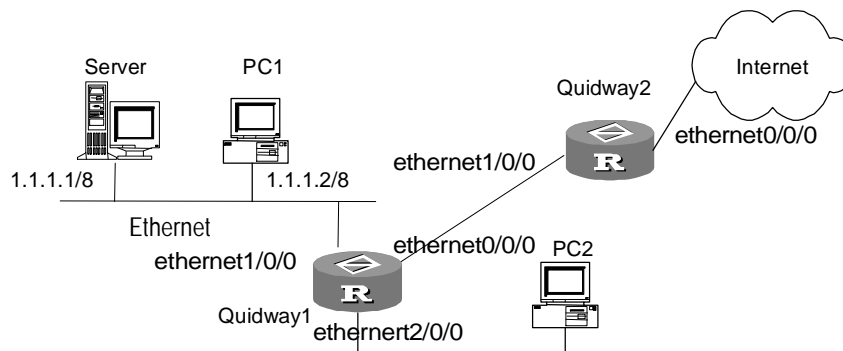


图2-5 流量监管、流量整形配置组网图

3. 配置步骤

(1) 配置路由器 Quidway1：

在 Quidway1 的 ethernet0/0/0 接口上配置 TS，对该接口发送的报文进行流量整形（对超过 0.5Mbps 的报文流进行整形），以降低在 Quidway2 接口 ethernet1/0/0 处的丢包率。


```
[Quidway1] interface ethernet0/0/0
[Quidway1-Ethernet0/0/0] qos gts any cir 500000
```

(2) 配置路由器 Quidway2:

配置 ACL 规则列表，分别匹配来源于 Server 和 PC1 的报文流。

```
[Quidway2] acl number 2001
[Quidway2-acl-basic-2001] rule permit source 1.1.1.1 0.0.0.0
[Quidway2] acl number 2002
[Quidway2-acl-basic-2002] rule permit source 1.1.1.2 0.0.0.0
```

在 ethernet1/0/0 接口上进行 TP 配置，对 ethernet1/0/0 接收到的不同报文流进行相应流量控制。

```
[Quidway2] interface ethernet1/0/0
[Quidway2-Ethernet1/0/0] qos car inbound acl 2001 cir 54000 cbs 54000 ebs 0
green pass red remark-prec-pass 0
[Quidway2-Ethernet1/0/0] qos car inbound acl 2002 cir 80000 cbs 80000 ebs 0
green pass red discard
[Quidway2-Ethernet1/0/0] qos car inbound any cir 500000 cbs 500000 ebs 0 green
pass red discard
```

在 ethernet0/0/0 接口上进行 TP 配置，对由 Ethernet 0/0/0 接口发送的报文进行流量控制，报文流量不能超过 1Mbps，如果超过流量限制则将违规报文丢弃。

```
[Quidway2] interface ethernet0/0/0
[Quidway2-Ethernet0/0/0] qos car outbound any cir 1000000 cbs 1000000 ebs 0
green pass red discard
```

第3章 拥塞管理

3.1 拥塞管理简介

对于网络单元，当分组到达的速度大于该接口发送分组的速度时，在该接口处就会产生拥塞。如果没有足够的存储空间来保存这些分组，它们其中的一部分就会丢失。分组的丢失又可能会导致发送该分组的主机或路由器因超时而重传此分组，这将导致恶性循环。

拥塞管理的中心内容就是当拥塞发生时如何制定一个资源的调度策略，决定报文转发的处理次序。

3.1.1 拥塞管理策略

对于拥塞管理，一般采用排队技术，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、延迟抖动等有着十分重要的影响。

这里介绍几种常用的队列调度机制。

1. FIFO（先进先出队列，First In, First Out Queuing）

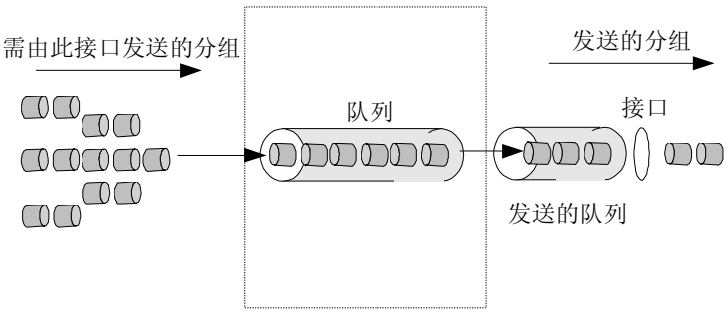


图3-1 先进先出队列示意图

如上图所示，FIFO 按照时间到达的先后决定分组的转发次序。用户的业务流在某个路由器能够获得的资源取决于分组的到达时机及当时的负载情况。Best-Effort 报文投递方式采用的就是 FIFO 的排队策略。

如果路由器的每个端口只有一个基于 FIFO 的输入或输出队列，那么恶性的应用可能会占用所有的网络资源，严重影响关键业务数据的传送。

每个队列内部报文的发送（次序）关系默认是 FIFO。

2. PQ (优先队列, Priority Queuing)

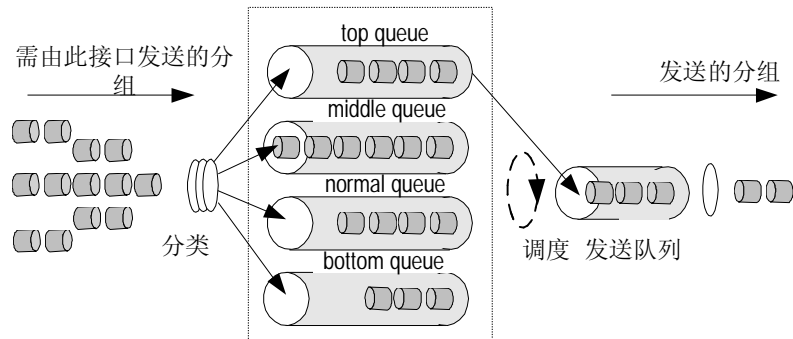


图3-2 优先队列示意图

PQ 队列是针对关键业务应用设计的。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。PQ 可以根据网络协议（比如 IP, IPX）、数据流入接口、报文长短、源地址/目的地址等灵活地指定优先次序。优先队列将报文分成 4 类，分别为高优先队列(top)、中优先队列(middle)、正常优先队列(normal)和低优先队列(bottom)，它们的优先级依次降低。缺省情况下，缺省数据流进入 normal 队列。

在队列调度时，PQ 严格按照优先级从高到低的次序，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。

PQ 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可能一直得不到服务。

3. CQ (定制队列, Custom Queuing)

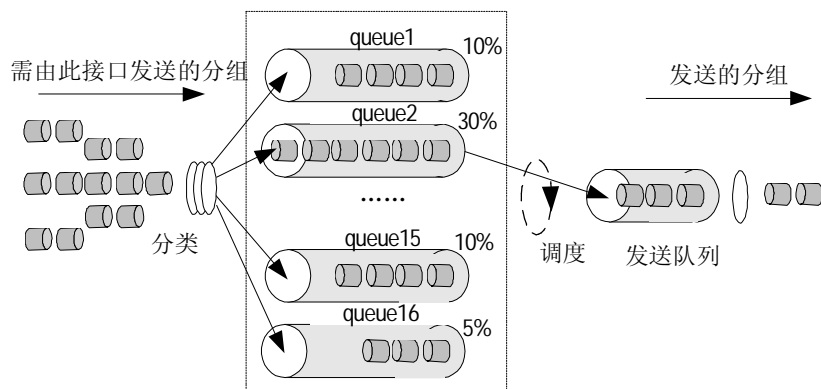


图3-3 定制队列示意图

CQ 按照一定的规则将分组分成 17 类（对应于 17 个队列），分组根据自己的类别按照先进先出的策略进入相应的 CQ 队列。

在 CQ 的 17 个队列中，0 号队列是系统队列（图中未画出），不允许用户配置；1 到 16 号队列是用户队列，如图 3-3 所示。用户可以配置流分类的规则，指定 16 个用户队列占用接口带宽的比例关系。在队列调度时，系统队列中的分组被优先发送。直到系统队列为空，再采用轮询的方式按照预先配置的带宽比例依次从 1 到 16 号用户队列中取出一定数量的分组发送出去。这样，就可以使不同业务的分组获得不同的带宽，既可以保证关键业务能获得较多的带宽，又不至于使非关键业务得不到带宽。缺省情况下，缺省数据流进入 1 号队列。

定制队列的另一个优点是：可根据业务的繁忙程度分配带宽，适用于对带宽有特殊需求的应用。虽然 16 个用户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。因此，当没有某些类别的报文时，CQ 调度机制能自动增加现存类别的报文可占的带宽。

4. WFQ（加权公平队列，Weighted Fair Queuing）

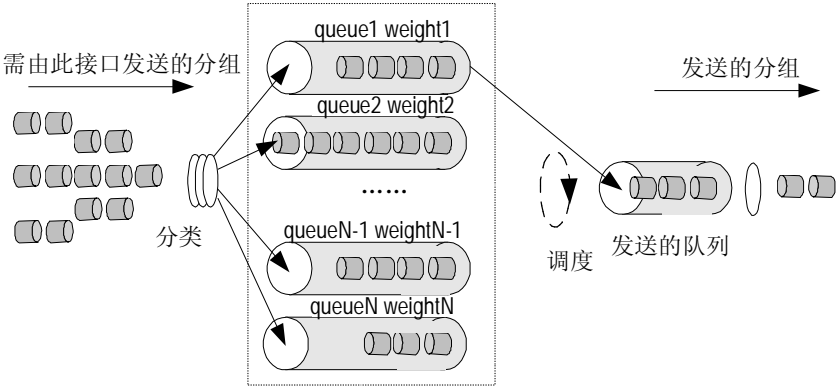


图3-4 加权公平队列示意图

在介绍加权公平队列前，先要理解公平队列 FQ（Fair Queue）。FQ 是为了公平地分享网络资源，尽可能使所有流的延迟和延迟抖动达到最优而推出的。它照顾了各方面的利益，主要表现在：

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

与 FQ 相比，WFQ 在计算报文调度次序时增加了优先权方面的考虑。从统计上，WFQ 使高优先权的报文获得优先调度的机会多于低优先权的报文。WFQ 能够按流的“会话”信息（包括协议类型、源和目的 TCP 或 UDP 端口号、源和目的 IP 地址及 ToS 域中的优先级位等）自动进行流分类，并且尽可能多地提供队列，以将每个流均匀地放入不同队列中，从而在总体上均衡各个流的延迟。在出队的时候，WFQ

按流的优先级 (precedence) 来分配每个流应占有出口的带宽。优先级的数值越小, 所得的带宽越少。优先级的数值越大, 所得的带宽越多。最后, 轮询各个队列, 按照带宽比例从队列中取出相应数量的报文进行发送。

例如: 接口中当前共有 5 个流, 它们的优先级分别为 0、1、2、3、4, 则带宽总配额为所有 (流的优先级+1) 的和。即

$$1 + 2 + 3 + 4 + 5 = 15$$

每个流所占带宽比例为: (自己的优先级数 + 1) / (所有 (流的优先级 + 1) 的和)。
即每个流可得的带宽分别为: 1/15, 2/15, 3/15, 4/15, 5/15。

由于 WFQ 在拥塞发生时能均衡各个流的延迟和延迟抖动, 所以 WFQ 在一些特殊场合得到了有效的应用。比如在使用资源预留协议 RSVP (Resource Reservation Protocol) 的保证型业务中, 通常就是采用 WFQ 作为调度策略; 在流量整形 TS 中, 也采用 WFQ 调度缓存的报文。

5. CBQ (基于类的队列, Class Based Queue)

CBQ 是对 WFQ 功能的扩展, 为用户提供了定义类的支持。CBQ 为每个用户定义类分配一个单独的 FIFO 预留队列, 用来缓冲同一类的数据。在网络拥塞时, CBQ 对输出报文根据用户定义类规则进行匹配, 并使其进入相应的队列, 在入队列之前必需进行拥塞避免机制 (尾部丢弃或 WRED, Weighted Random Early Detection, 加权随机早期检测) 和带宽限制的检查。在报文出队列时, 加权公平调度每个类对应的队列中的报文。

CBQ 提供一个紧急队列, 紧急报文入紧急队列, 该紧急队列采用 FIFO 调度, 没有带宽限制。这样, 如果 CBQ 加权公平对待所有类的队列, 语音报文这类对延迟敏感的数据流就可能不能及时发送。为此将 PQ 特性引入 CBQ, 称其为 LLQ (Low Latency Queueing, 低延迟队列), 为语音报文这样的对延迟敏感的数据流提供严格优先发送服务。

LLQ 将严格优先队列机制与 CBQ 结合起来使用, 用户在定义类时可以指定其享受严格优先服务, 这样的类称作优先类。所有优先类的报文将进入同一个优先队列, 在入队列之前需对各类报文进行带宽限制的检查。报文出队列时, 将首先发送优先队列中的报文, 直到发送完后才发送其他类对应的队列的报文。在发送其他队列报文时将仍然按照加权公平的方式调度。

为了不让其他队列中的报文延迟时间过长, 在使用 LLQ 时将会为每个优先类指定可用最大带宽, 该带宽值用于拥塞发生时监管流量。如果拥塞未发生, 优先类允许使用超过分配的带宽。如果拥塞发生, 优先类超过分配带宽的数据包将被丢弃。LLQ 还可以指定 Burst-size。

系统在为报文匹配规则时, 总是先匹配优先类, 然后再匹配其他类, 对多个优先类, 按照配置顺序逐一匹配, 对其他类, 也是按照配置顺序逐一匹配, 对类中多个规则, 按照配置顺序逐一匹配。

6. RTP（Real-time Transport Protocol）优先队列

RTP 优先队列是一种解决实时业务（包括语音与视频业务）服务质量的简单的队列技术。其原理就是将承载语音或视频的 RTP 报文送入高优先级队列，使其得到优先发送，保证时延和抖动降低为最低限度，从而保证了语音或视频这种对时延敏感业务的服务质量。

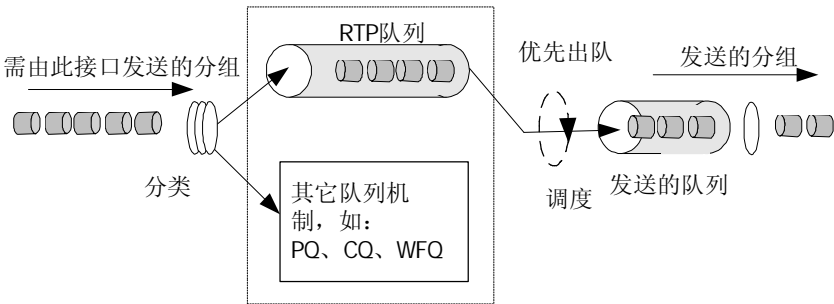


图3-5 RTP 队列示意图

如上图所示，RTP 优先队列将 RTP 报文送入一个具有较高优先级的队列。RTP 报文是端口号在一定范围内为偶数的 UDP 报文，端口号的范围可以配置。RTP 优先队列可以同任何一种队列（包括 FIFO、PQ、CQ、WFQ 与 CBQ）结合使用，而它的优先级是最高的。但由于 CBQ 中的 LLQ 也可以解决实时业务，所以一般不推荐将 RTP 优先队列与 CBQ 结合应用。

3.1.2 拥塞管理技术的对比

Quidway 路由器提供了以上拥塞管理技术。突破了传统 IP 设备的单一 FIFO 拥塞管理策略，提供了强大的 QoS 能力，使得 IP 设备可以满足不同业务所要求的不同服务质量的要求。为了更好的利用拥塞管理技术，现对各种队列技术做一比较。

表3-1 拥塞管理技术对比

类型	队列数	优点	缺点
FIFO	1	1、不需要配置，易于使用。 2、处理简单，延迟小。	1、所有的报文，无论紧急与否，语音还是数据，均进入一个“先进先出”的队列，发送报文所占用的带宽、延迟时间、丢失的概率均由报文到达队列的先后顺序决定。 2、对不配合的数据源（即没有流控机制的流，如 UDP 报文发送）无约束力，不配合的数据源会造成配合的数据源（如 TCP 报文发送）带宽受损失。 3、对时间敏感的实时应用（如 VoIP）的延迟得不到保证。

类型	队列数	优点	缺点
PQ	4	可对不同业务的数据提供绝对的优先，对时间敏感的实时应用（如 VoIP）的延迟可以得到保证。对优先业务的报文的带宽占用可以绝对优先。	1、需配置，处理速度慢。 2、如果不对高优先级的报文的带宽加限制，会造成低优先级的报文得不到带宽。
CQ	16	1、可对不同业务的报文按带宽比例分配带宽。 2、当没有某些类别的报文时，能自动增加现存类别的报文可占的带宽。	需配置，处理速度慢
WFQ	可配置	1、配置容易。 2、可以保护配合（交互）的数据源（如 TCP 报文发送）的带宽。 3、可以减小延迟抖动。 4、可以减小数据量小的交互式应用的延迟。 5、可以为不同优先级的流分配不同的带宽。 6、当流的数目减少时，能自动增加现存流可占的带宽。	处理速度比 FIFO 要慢。但比 PQ、CQ 要快。
CBQ	可配置 (0~64)	1、可以对数据根据灵活、多样的分类规则进行划分，分别为 EF（加速转发）、AF（确保转发）、BE（尽力转发）业务提供不同的队列调度机制。 2、可以为 AF 业务提供严格、精确的带宽保证，并且保证各类 AF 业务之间根据权重按一定的比例关系进行队列调度。 3、可以为 EF 业务提供绝对优先的队列调度，确保实时数据的时延；同时通过对高优先级数据流量的限制，克服了 PQ 的低优先级队列可能“饿死”的弊病。 4、对于尽力转发的缺省类数据，提供 WFQ 队列调度。	系统开销比较大

3.2 先进先出队列的配置

先进先出队列 FIFO 的配置包括：

- 1 配置 FIFO 队列的长度

3.2.1 配置 FIFO 队列的长度

FIFO 是接口缺省使用的队列调度机制，可以通过配置命令改变其队列长度。
请在接口视图下进行下列配置。

表3-2 配置 FIFO 队列的长度

操作	命令
配置 FIFO 队列的长度	qos fifo queue-length <i>queue-length</i>
恢复 FIFO 队列的缺省长度	undo fifo queue-length

FIFO 队列的缺省长度为 75。

3.3 优先队列的配置

优先队列 PQ 的配置包括：

- 配置优先列表
- 在接口上应用优先列表组

3.3.1 配置优先列表

1. 根据网络层协议配置优先列表

根据协议类型对分组进行分类，使之进入不同的队列。对于同一个 *pql-index*，本命令的重复使用可以为 *pql-index* 建立多个规则。
系统以规则被配置的顺序来匹配分组，如果发现分组与某个规则匹配，便结束整个查找过程。
请在系统视图下进行下列配置。

表3-3 根据网络层协议配置优先列表

操作	命令
根据网络层协议配置优先列表	qos pql <i>pql-index protocol protocol-name queue-key key-value queue { top middle normal bottom }</i>
删除 <i>pql-index</i> 中相应的分类规则	undo qos pql <i>pql-index protocol protocol-name queue-key key-value queue { top middle normal bottom }</i>

2. 根据分组来自的接口配置优先列表

根据分组来自的路由器接口进行分类，使之进入不同的队列。
请在系统视图下进行下列配置。

表3-4 根据接口配置优先列表

操作	命令
根据分组来自的接口配置优先列表	qos pql pql-index inbound-interface interface-type interface-number queue { top middle normal bottom }
删除 <i>pql-index</i> 中相应的分类规则	undo qos pql pql-index inbound-interface interface-type interface-number

3. 配置缺省队列

为不与任何规则匹配的包指定一个缺省队列。

请在系统视图下进行下列配置。

表3-5 配置缺省队列

操作	命令
配置缺省队列	qos pql pql-index default-queue { top middle normal bottom }
恢复缺省队列的缺省值	undo qos pql pql-index default-queue

可以给一个优先列表的组定义多条规则，然后把该组规则应用在某接口上。当一个分组到达该接口时（需要由此接口传出去），系统沿规则链匹配该分组，如果匹配上某规则，则进入相应的队列，匹配结束；如果分组不与任何规则匹配，则进入缺省队列。

缺省队列的缺省值为 **normal**。

4. 配置队列长度

设置各队列的长度（即队列所能容纳的分组的个数）。

请在系统视图下进行下列配置。

表3-6 配置队列长度

操作	命令
配置队列长度	qos pql pql-index queue { top middle normal bottom } queue-length queue-length
形式恢复各队列长度的缺省值	undo qos pql pql-index queue { top middle normal bottom } queue-length

各队列的缺省长度如下表所示。

表3-7 队列缺省长度

队列	长度
top	20
middle	40
normal	60
bottom	80

3.3.2 在接口上应用优先列表组

将一组优先列表应用到接口上。对于同一个接口，本命令的重复使用将为接口设定新的优先列表组。

请在接口视图下进行下列配置。

表3-8 在接口上应用优先列表组

操作	命令
在接口上应用优先列表组	qos pq pql <i>pql-index</i>
取消使用 PQ	undo qos pq

缺省情况下，接口不使用 PQ，而使用 FIFO。



注意：

除链路层使用 X.25 及 LAPB 的接口外，所有物理接口都可以应用 PQ。

3.3.3 优先队列的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示优先列表及在接口上的应用情况，通过查看显示信息验证配置的效果。

表3-9 显示优先列表及在接口上的应用情况

操作	命令
显示优先列表的状态	display qos pql [<i>pql-index</i>]
显示接口上优先列表的配置情况	display qos pq interface [<i>interface-type</i> <i>interface-number</i>]

3.4 定制队列的配置

定制队列 CQ 的配置包括：

- 配置定制列表
- 在接口上应用定制列表组

3.4.1 配置定制列表

定制列表共可分为 16 个组（1~16），每个组指明了什么样的分组进入什么样的队列、各队列的长度和每次轮询各队列所能连续发送的字节数等信息。在一个接口上只能应用一个定制列表。

1. 根据网络层协议配置定制列表

根据协议类型对分组进行分类，使之进入不同的队列。目前，VRP 只支持对 IP 报文进行分类。

请在系统视图下进行下列配置。

表3-10 根据网络层协议配置定制列表

操作	命令
根据网络层协议配置定制列表	qos cql <i>cql-index</i> protocol <i>protocol-name</i> <i>queue-key</i> <i>key-value</i> queue <i>queue-number</i>
删除 <i>cql-index</i> 中相应的分类规则	undo qos cql <i>cql-index</i> protocol <i>protocol-name</i> <i>queue-key</i> <i>key-value</i>

2. 根据分组来自的接口配置定制列表

建立基于接口的分类规则。对于同一个 *cql-index*，本命令的重复使用可以为 *cql-index* 增加新的规则。

请在系统视图下进行下列配置。

表3-11 根据接口配置定制列表

操作	命令
根据分组来自的接口配置定制列表	qos cql <i>cql-index</i> inbound-interface <i>interface-type</i> <i>interface-number</i> queue <i>queue-number</i>
删除 <i>cql-index</i> 中相应的分类规则	undo qos cql <i>cql-index</i> inbound-interface <i>interface-type</i> <i>interface-number</i>

3. 配置缺省队列

为那些不与任何规则匹配的分组指定一个缺省队列。

请在系统视图下进行下列配置。

表3-12 配置缺省队列

操作	命令
配置缺省队列	qos cql cql-index default-queue queue-number
恢复缺省队列的缺省值	undo qos cql cql-index default-queue

我们可以给一个定制列表的组定义多条规则，然后把该组应用在某接口上。当一个分组到达该接口时（由此接口传送出去），系统沿规则链匹配该分组，如果匹配上某规则，则进入相应的队列，匹配结束；如果分组不与任何规则匹配，则进入缺省队列。

缺省队列的缺省值为 1。

4. 配置队列长度

设置各定制队列的长度（即队列所能容纳的分组的个数）。

请在系统视图下进行下列配置。

表3-13 配置队列长度

操作	命令
配置队列长度	qos cql cql-index queue queue-number queue-length queue-length
恢复各队列长度的缺省值	undo qos cql cql-index queue queue-number queue-length

其中：*queue-length* 为队列的最大长度，缺省值为 20。

5. 配置队列连续发送字节数

设置各队列每次轮询所发送分组的字节数。

请在系统视图下进行下列配置。

表3-14 配置队列连续发送字节数

操作	命令
配置连续发送字节数	qos cql cql-index queue queue-number serving byte-count
恢复发送字节数的缺省值	undo qos cql cql-index queue queue-number serving

其中：

byte-count: 当路由器调度 CQ 的用户队列时，它连续从这个队列中取出分组进行发送，直到发送的字节数不少于为该队列配置的 *byte-count* 的值或者队列为空，再转而调度 CQ 的下一个用户队列。因此，*byte-count* 的值会影响 CQ 各用户队列之间

占用接口带宽的比例关系，并且决定了多长时间路由器才会调度 CQ 的下一个队列。
byte-count 的缺省字节数为 1500。

如果 *byte-count* 的值过小，由于路由器每次至少发送一个分组才会转向下一个队列，各个队列实际获得的带宽很可能与预想的效果相差甚远；如果 *byte-count* 值过大，则可能会造成队列间切换延迟太大。

3.4.2 在接口上应用定制列表

请在接口视图下进行下列配置。

表3-15 在接口上应用定制列表

操作	命令
在接口上应用定制列表	qos cq cql cql-index
取消使用 CQ	undo qos cq

缺省情况下，接口不使用 CQ，而使用 FIFQ。



注意：

除链路层使用 X.25 及 LAPB 的接口外，所有物理接口都可以应用 CQ。

3.4.3 定制队列的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示定制列表状态及在接口上的应用情况，通过查看显示信息验证配置的效果。

表3-16 显示定制列表状态及在接口上的应用情况

操作	命令
显示定制列表状态	display qos cql
显示定制列表在接口上应用情况	display qos cq interface [interface-type interface-number]

3.5 加权公平队列的配置

加权公平队列 WFQ 的配置包括：

- 1 在接口上应用加权公平队列

3.5.1 在接口上应用加权公平队列

当接口没有使用 WFQ 策略时，使用本命令可以使接口使用 WFQ 策略，同时可指定 WFQ 的参数。如果接口已经使用了 WFQ 策略，使用本命令可以修改 WFQ 的参数。请在接口视图下进行如下配置。

表3-17 使用加权公平队列或修改 WFQ 的参数

操作	命令
使用加权公平队列或修改 WFQ 的参数	qos wfq [queue-length <i>max-queue-length</i> [queue-number <i>total-queue-number</i>]]
取消使用 WFQ	undo qos wfq

缺省情况下，接口不使用 WFQ，而使用 FIFO。



注意：

除链路层使用 X.25 及 LAPB 的接口外，所有物理接口都可以应用加权公平队列。

3.5.2 加权公平队列的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示接口加权公平队列的配置情况和统计信息，通过查看显示信息验证配置的效果。

表3-18 显示接口加权公平队列的配置情况和统计信息

操作	命令
显示接口加权公平队列的配置情况和统计信息	display qos wfq interface [<i>interface-type interface-number</i>]

3.6 基于类的队列的配置

基于类的队列 CBQ 的配置包括：

- | 配置接口最大可用带宽
- | 定义类，并在类视图中定义一组流分类规则
- | 定义流行为，并在流行为视图中定义一组 QoS 特性
- | 定义策略，在策略视图下为使用的类中指定对应的流行为
- | 在接口或 ATM PVC 视图下应用 QoS 策略

为方便用户使用，系统预定义了一些类、流行为以及策略，具体如下。

1. 系统预定的类

系统预定义了一些类，并为这些类定义了通用的规则，用户定义策略时可直接使用这些类，这些类包括：

(1) 缺省类

default-class: 匹配的是缺省数据流。

(2) 基于 DSCP 的预定义类

ef、af1、af2、af3、af4: 分别匹配 IP DSCP 值 ef、af1、af2、af3、af4

(3) 基于 IP 优先级的预定义类

ip-prec0, ip-prec1, ...ip-prec7: 分别匹配 IP 优先级 0, 1, ...7

(4) 基于 MPLS EXP 的预定义类

mpls-exp0, mpls-exp1, ...mpls-exp7: 分别匹配 MPLS EXP 值 0, 1, ...7

2. 系统预定义的流行为

系统预定义了一些流行为，并为这些流行为定义了 QoS 特性：

(1) **ef:** 定义了一个特性为入 EF 队列，占用带宽为接口可用带宽的 20%

(2) **af:** 定义了一个特性为入 AF 队列，占用带宽为接口可用带宽的 20%

(3) **be:** 不定义任何特性

3. 系统预定义的策略

系统预定义了一个策略，为该策略指定了使用的预定义类，并为这些类指定预定义的动作。该策略名为 **default**，具有缺省的 CBQ 动作。

default 策略的具体规则如下：

(1) 预定义类 **ef**，采用预定义流行为 **ef**

(2) 预定义类 **af1~af4**，采用预定义流行为 **af**

(3) **default-class** 类，采用预定义流行为 **be**

3.6.1 配置接口最大可用带宽

该带宽指 CBQ 中报文入队列带宽检查时使用的最大接口带宽，并非指物理接口的实际带宽。

请在接口视图下进行下列配置。

表3-19 配置 MP 绑定带宽

操作	命令
配置本接口的带宽	qos max-bandwidth <i>bandwidth</i>
恢复本接口的带宽缺省值	undo qos max-bandwidth

bandwidth 是接口的可用带宽，单位 Kbps，范围为 1 到 1000000。缺省情况下，对于物理接口，其取值为物理接口实际的波特率或速率；对于 T1/E1、MFR 等通过绑定生成的逻辑串口，其取值为绑定通道的总带宽；对于虚拟接口模板（Virtual Template）、VE 等逻辑接口，取值为 64Kbps。

建议该值小于物理接口或逻辑链路的实际可用带宽。对于串口该值缺省为 64kbps，可以先通过 **baudrate** 命令修改串口速率后（如改为 2.048Mbps）后再重新设定该值（如设为 115.2kbps）。

3.6.2 定义类并配置其匹配规则

定义类首先要创建一个类名称，然后在此类视图下配置其匹配规则。

1. 定义类并进入类视图

请在系统视图下进行下列配置。

表3-20 定义一个类并进入类视图

操作	命令
定义类并进入类映射视图	traffic classifier <i>tcl-name</i> [operator { and or }]
删除类并进入类映射视图	undo traffic classifier <i>tcl-name</i>

用户定义的类型 *tcl-name* 不允许为系统预定义类。

缺省为 **and**，即类视图下各匹配规则之间的关系为逻辑与。

2. 定义或删除匹配所有数据包的规则

请在类视图下进行下列配置。

表3-21 定义或删除匹配所有数据包的规则

操作	命令
定义匹配所有数据包的规则	if-match [not] any
删除匹配所有数据包的规则	undo if-match [not] any

3. 定义或删除 classifier 匹配规则

请在类视图下进行下列配置。

表3-22 定义或删除 classifier 匹配规则

操作	命令
定义 classifier 匹配规则	if-match [not] classifier <i>tcl-name</i>
删除 classifier 匹配规则	undo if-match [not] classifier <i>tcl-name</i>

该命令不能递归使用，例如，traffic classifier A 定义了匹配 traffic classifier B 的规则，traffic classifier B 不能再直接或者间接的引用 traffic classifier A。

4. 定义或删除 ACL 匹配规则

定义 ACL 匹配规则。

请在类视图下进行下列配置。

表3-23 定义或删除 ACL 匹配规则

操作	命令
定义 ACL 匹配规则	if-match [not] acl <i>access-list-number</i>
删除 ACL 匹配规则	undo if-match [not] acl <i>access-list-number</i>

5. 定义或删除 MAC 地址匹配规则

请在类视图下进行下列配置。

表3-24 定义或删除目的 MAC 地址匹配规则

操作	命令
定义 MAC 地址匹配规则	if-match [not] { destination-mac source-mac } <i>mac-address</i>
删除 MAC 地址匹配规则	undo if-match [not] { destination-mac source-mac } <i>mac-address</i>

目的 MAC 地址匹配规则只对出方向的策略有意义，并且只对以太类型的接口有意义。

源 MAC 地址匹配规则只对入方向的策略有意义，并且只对以太类型的接口有意义。

6. 定义或删除类的入接口匹配规则

请在类视图下进行下列配置。

表3-25 定义或删除类的入接口匹配规则

操作	命令
定义类的入接口匹配规则	if-match [not] inbound-interface <i>type number</i>
删除类的入接口匹配规则	undo if-match [not] inbound-interface <i>type number</i>

匹配的接口删除时，该规则自动删除。

7. 定义或删除 DSCP 匹配规则

DSCP（Differentiated Services CodePoint，差分服务编码点）是 IETF DiffServ 工作组将 IP 报文头 ToS 字节的高 6 位重新定义的域，ToS 字节因而也改名为 DS 字节。在 DiffServ 方案中，在网络入口处根据服务要求对业务进行分类、流量控制，同时设置 DSCP，在网络中将依据分组的 DSCP 值来区分每一类通信并为之服务（包括资源分配、分组丢弃策略等）。

用户可以根据 DSCP 值来设置分类的匹配规则。

请在类视图下进行下列配置。

表3-26 定义或删除 DSCP 匹配规则

操作	命令
定义 DSCP 匹配规则	if-match [not] dscp { <i>dscp-value</i> }
删除 DSCP 匹配规则	undo if-match [not] dscp { <i>dscp-value</i> }

8. 定义或删除 IP 优先值匹配规则

请在类视图下进行下列配置。

表3-27 定义或删除 IP 优先值匹配规则

操作	命令
定义 IP 优先值匹配规则	if-match [not] ip-precedence { <i>ip-precedence-value</i> }
删除 IP 优先值匹配规则	undo if-match [not] ip-precedence

配置时将需要配置的 IP 优先值用一条命令进行配置，否则最后配置的 **if-match ip-precedence** 命令会覆盖前面的配置。

9. 定义或删除 RTP 协议端口匹配规则

请在类视图下进行下列配置。

表3-28 定义或删除 RTP 协议端口匹配规则

操作	命令
定义 RTP 协议端口匹配规则	if-match [not] rtp start-port <i>starting-port-number</i> end-port <i>end-port-number</i>
删除 RTP 协议端口匹配规则	undo if-match [not] rtp

由于 RTP 队列优先于 CBQ，所以如果同时配置了 RTP 队列与基于匹配 RTP 协议的类的调度队列，只有 RTP 队列生效。

10. 定义或删除协议匹配规则

请在类视图下进行下列配置。

表3-29 定义或删除协议匹配规则

操作	命令
定义协议匹配规则	if-match [not] protocol <i>protocol-name</i>
删除协议匹配规则	undo if-match [not] protocol <i>protocol-name</i>

其中 *protocol-name* 为 IP 协议。

3.6.3 定义流行为并配置其特性

定义流行为首先需要创建一个流行为名称，然后在此流行为视图下配置其特性。

1. 定义流行为并进入流行为视图

请在系统视图下进行下列配置。

表3-30 定义一个流行为并进入流行为视图

操作	命令
定义一个流行为并进入流行为视图	traffic behavior <i>behavior-name</i>
删除流行为	undo traffic behavior <i>behavior-name</i>

behavior-name: 流行为名，不允许为系统预定义流行为。

2. 配置确保转发（AF），并配置最小可保证带宽

请在流行为视图下进行下列配置。

表3-31 配置确保转发 (AF)，并配置最小可保证带宽

操作	命令
配置确保转发 (AF)，并配置最小可保证带宽	queue af bandwidth { <i>bandwidth</i> pct percentage }
删除确保转发配置	undo queue af

该行为只能应用在接口和 ATM PVC 的出方向。

在同一流行为下需要用同一单位配置 **queue ef** 和 **queue af**，或者用 *bandwidth*，或者用百分比进行配置。

AF 可以保证在应用向网络发送的业务流量没有超过约定值的情况下，该应用的报文丢失概率非常低，AF 有 4 类，每一类可以设置 3 个不同的丢弃优先级。

3. 配置加速转发 (EF)，并配置最大带宽

请在流行为视图下进行下列配置。

表3-32 配置加速转发 (EF)，并配置最大带宽

操作	命令
配置加速转发 (EF)，并配置最大带宽	queue ef bandwidth { <i>bandwidth</i> [<i>cbs committed-burst-size</i>] pct percentage [<i>cbs_ratio ratio</i>] }
取消该配置	undo queue ef

该命令在流行为视图下不能与 **queue af**、**queue-length**、**wred** 同时使用。

缺省类不能与包含该命令的行为关联。

在同一策略下各个类需用同一单位配置 **queue ef** 和 **queue af**，或者用 *bandwidth*，或者用百分比进行配置。

EF 用于支持低丢失率、低时延、确保带宽的应用。

4. 配置采用公平队列

请在流行为视图下进行下列配置。

表3-33 配置采用公平队列

操作	命令
配置采用公平队列	queue wfq [<i>queue-number total-queue-number</i>]
取消采用公平队列的配置	undo queue wfq

配置了该特性的流行为仅可以与缺省类关联使用。

5. 配置最大队列长度

配置最大队列长度，丢弃方式为尾丢弃。

请在流行为视图下进行下列配置。

表3-34 配置最大队列长度

操作	命令
配置最大队列长度	queue-length <i>queue-length</i>
取消最大队列长度的配置	undo queue-length <i>queue-length</i>

该命令必须在配置了 **queue af** 和 **queue wfq** 后使用；执行 **undo queue af** 或 **undo queue wfq** 命令，则 **queue-length** 也同时被取消。

如果是缺省类，必须在配置了 **queue af** 或 **queue wfq** 后使用。

6. 配置丢弃方式为随机丢弃方式

请在流行为视图下进行下列配置。

表3-35 配置丢弃方式为随机丢弃方式

操作	命令
配置丢弃方式为随机丢弃方式	wred [dscp ip-precedence]
恢复缺省配置	undo wred [dscp ip-precedence]

dscp: 表明在为一个包计算丢弃概率时使用的是 DSCP 值。

ip-precedence: 表明在为一个包计算丢弃概率时使用的是 IP 优先级值，作为缺省配置。

该命令必须在配置了 **queue af** 或 **queue wfq** 后使用。**wred** 和 **queue-length** 是互斥的。删除时将删除在该随机丢弃下的其他配置。当接口上应用了包含 WRED 特性的 QoS 策略后，原有的接口级的 WRED 配置失效。

缺省类 **default-class** 只能与配置基于 IP 优先级的随机丢弃方式的行为关联。

7. 设置 WRED 计算平均队列长度的指数

请在流行为视图下进行下列配置。

表3-36 设置 WRED 计算平均队列长度的指数

操作	命令
配置 WRED 计算平均队列长度的指数	wred weighting-constant <i>exponent</i>
取消 WRED 计算平均队列长度的指数的配置	undo wred weighting-constant

需配置了 **queue af**，并已用 **wred** 使能了 WRED 丢弃方式后才可以配置该命令。

8. 配置 WRED 各 DSCP 的下限、上限和丢弃概率分母

请在流行为视图下进行下列配置。

表3-37 设置 WRED 各 DSCP 的下限、上限和丢弃概率分母

操作	命令
配置 WRED 各 DSCP 的下限、上限和丢弃概率分母	wred dscp <i>dscp-value</i> low-limit <i>low-limit</i> high-limit <i>high-limit</i> [discard-probability <i>discard-prob</i>]
取消 WRED 各 DSCP 的下限、上限和丢弃概率分母的配置	undo wred dscp <i>dscp-value</i>

dscp-value: DSCP 值，取值范围为 0~63，或可以是如下关键字 **ef**, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs7** 或 **default**。

需已用 **wred dscp** 使能了基于 DSCP 的 WRED 丢弃方式。

取消 **wred** 配置，**wred dscp** *dscp-value* 配置同时被取消。

取消 **queue af** 配置，丢弃参数的配置同时被取消。

9. 配置 WRED 各优先级的下限、上限和丢弃概率分母

请在流行为视图下进行下列配置。

表3-38 配置 WRED 各优先级的下限、上限和丢弃概率分母

操作	命令
设置 WRED 各优先级的下限、上限和丢弃概率分母	wred ip-precedence <i>precedence</i> low-limit <i>low-limit</i> high-limit <i>high-limit</i> [discard-probability <i>discard-prob</i>]
取消 WRED 各优先级的下限、上限和丢弃概率分母的配置	undo wred ip-precedence <i>precedence</i>

需已用 **wred ip-precedence** 使能了基于优先级的 WRED 丢弃方式。

取消 **wred** 配置，**wred ip-precedence** 配置同时被取消。

取消 **queue af** 配置，丢弃参数的配置同时被取消。

10. 配置使用或取消流量监管

请在流行为视图下进行下列配置。

表3-39 配置使用或取消流量监管

操作	命令
配置使用流量监管	car cir committed-information-rate [cbs committed-burst-size ebs excess-burst-size] [green action [red action]]
配置取消流量监管	undo car

其中：**action** 是对数据包采取的动作，有以下几种：

- | **discard**: 丢弃数据包
- | **pass**: 发送数据包。
- | **remark-dscp-pass new-dscp**: 设置新的 DSCP 值 new-dscp，并发送。取值范围为 0~63。
- | **remark-prec-pass new-prec**: 设置新的 IP 优先级 new-prec，并发送。取值范围为 0~7。
- | **remark-mpls-exp-pass new-exp**: 设置新的 mpls exp，并发送。取值范围为 0~7。

策略中的类关联了包含 TP 特性的行为时，可以应用到接口的入或出方向。

策略中的类关联了包含 TP 特性的行为时，将导致接口上原有的 **qos car** 命令失效。

如果多次使用本命令在同一个流行为上配置，最后一次配的将覆盖前面配的。

使用流量监管但未使用 AF 或 EF 配置的类，如果通过了监管的检测可以发送，但却遇到接口拥塞，则将进入缺省队列。

11. 配置使用或取消流量整形

请在流行为视图下进行下列配置。

表3-40 配置使用或取消流量整形

操作	命令
配置使用流量整形	gts cir committed-information-rate [cbs committed-burst-size [ebs excess-burst-size [queue-length queue-length]]]
配置取消流量整形	undo gts

接口上应用的类策略中使用具有 **gts** 的流行为时，只能应用到接口的出方向。

接口上应用包含 TS 的类策略，将导致接口上原有的 **qos gts** 命令失效。

如果多次使用本命令在同一个流行为上配置，最后一次的配置将覆盖前面的配置。

使用流量监管但未使用 AF 或 EF 配置的类，如果通过了整形的检测可以发送，但却遇到接口拥塞，则将进入缺省队列。

12. 配置使用或取消流量限速

请在流行为视图下进行下列配置。

表3-41 配置使用或取消流量限速

操作	命令
配置使用流量限速	lr cir committed-information-rate [cbs committed-burst-size [ebs excess-burst-size]] 或 lr percent cir committed-information-rate [cbs committed-burst-size [ebs excess-burst-size]]
配置取消流量限速	undo lr

策略中使用具有 **lr** 的行为时，只能应用到接口的出方向。

如果多次使用本命令在同一个行为上配置，后一次的配置将覆盖前面的配置。

在策略嵌套中配置限速，请遵循下面原则：

- 1. 父策略中必须先配置限速（通过 **lr** 或 **lr percent** 命令配置），子策略中才能配置队列。若子策略中配置了队列，使用子策略中的队列长度（**qos gts** 命令配置）。如果父策略中配置了限速且子策略中没有配置队列，则限速使用 **FIFO** 队列，队列长度取固定值 200。子策略配置队列后，父策略中相应的限速不允许删除。
- 2. 若父策略中配置的是 **lr** 命令，子策略的队列可以配置 **lr** 命令或 **lr percent** 命令形式；若父策略中配置的是 **lr percent** 命令，子策略中必须配置 **lr percent** 命令形式。

在 **ATM** 和 **FR** 接口上配置限速，请注意以下几点：

- 1. **LR** 特性不能被应用在 **ATM** 接口上，只能被应用在 **ATM PVC** 上。
- 2. **FR PVC** 上只能配置 **lr**，不允许配置 **lr percent**。
- 3. **FR** 接口如果配置了 **fr traffic-shaping**，则接口策略中不允许再配置 **LR**。

13. 配置标记报文的 DSCP 值

请在流行为视图下进行下列配置。

表3-42 配置标记报文的 DSCP 值

操作	命令
配置标记报文的 DSCP 值	remark dscp dscp-value
取消标记报文的 DSCP 值的配置	undo remark dscp

14. 配置标记报文的 IP 优先级值

请在流行为视图下进行下列配置。

表3-43 配置标记报文的 IP 优先级值

操作	命令
配置标记报文的 IP 优先级值	remark ip-precedence <i>ip-prec-value</i>
取消标记报文的 IP 优先级值的配置	undo remark ip-precedence

15. 配置标记 VLAN 报文的 802.1p 优先级值

请在流行为视图下进行下列配置。

表3-44 配置标记 VLAN 报文的 802.1p 优先级值

操作	命令
配置标记 VLAN 报文的 802.1p 优先级值	remark dot1p <i>cos-value</i>
取消标记 VLAN 报文的 802.1p 优先级值的配置	undo remark dot1p

16. 配置标记 FR 报文的 DE 标志位的值

请在流行为视图下进行下列配置。

表3-45 配置标记 FR 报文的 DE 标志位的值

操作	命令
配置标记 FR 报文的 DE 标志位的值	remark fr-de <i>fr-de-value</i>
取消标记 FR 报文的 DE 标志位的值的配置	undo remark fr-de

17. 配置标记 ATM 报文的 CLP 标志位

表3-46 配置标记 ATM 报文的 CLP 标志位

操作	命令
配置标记 ATM 报文的 CLP 标志位	remark atmclp <i>atmclp-value</i>
取消标记 ATM 报文的 CLP 标志位的值	undo remark atmclp

该行为只能应用在接口和 ATM PVC 的出方向。

18. 配置使用或取消策略嵌套

通过在行为下应用子策略，可以实现策略嵌套功能。即由 **traffic classifier** 命令定义的某一类流量除了执行父策略中定义的行为外，还由子策略再对该类流量进行分

类，并执行子策略中定义的行为。可以参考典型配置举例中的策略嵌套配置举例来理解策略嵌套的功能。

请在流行为视图下进行下列配置。

表3-47 配置使用或取消策略嵌套

操作	命令
配置使用策略嵌套	traffic-policy <i>policy-name</i>
配置取消策略嵌套	undo traffic-policy

配置策略嵌套功能，请注意以下几点：

- 1. 策略嵌套功能只支持二层嵌套。
- 1. 如果父策略和子策略中都配置了 **REMARK** 行为，则子策略中的 **REMARK** 会覆盖掉父策略中的 **REMARK**。如果父策略和子策略中都配置了 **CAR**（或 **GTS**），则 **CAR**（或 **GTS**）被执行两遍，子策略中的 **CAR**（或 **GTS**）会先被执行。如果父策略和子策略都配置了队列（此时父策略必然配置了限速），则限速（**LR**）不通过的报文进入子策略的队列，**LR** 通过的报文再经过父策略的队列调度。
- 1. 当子策略中配置了 **queue ef**，**queue af**，**queue wfq** 行为，即子策略为 **CBQ** 策略时，父策略中对应的类必须应用了 **LR** 行为。
- 1. 策略嵌套可以应用到物理接口、子接口、**FR PVC** 和 **ATM PVC** 上。
- 1. 嵌套策略既可以应用在接口（或 **PVC**）的入方向上，也可以应用在出方向上。对于接口上的子策略，入方向不能配置 **LR**、**CBQ**、**GTS**、**remark fr-de** 和 **remark atm-clp**；出方向不能配置 **remark fr-de** 和 **remark atm-clp**；**remark 8021p** 只能配置在以太网接口上（不含 **VE** 接口）；**CBQ** 不能配置在 **ATM** 物理接口（只能配置在 **ATM PVC** 上）、**VE** 接口、子接口上。

3.6.4 配置策略

1. 定义策略并进入策略视图

策略映射定义该策略中每个类的流行为，而每个流行为由一组特性要求组成，例如队列调度，包括 **EF**，**AF**，**WFQ**，流量监管（**TP**），流量整形（**TS**），**WRED**、标记等等。

请在系统视图下 进行下列配置。

表3-48 定义策略并进入策略视图

操作	命令
定义策略并进入策略视图	qos policy <i>policy-name</i>
删除指定策略	undo qos policy <i>policy-name</i>

策略名不允许是系统预定义策略。

策略创建时，缺省具有缺省类 **default-class**，该类关联 **be** 行为。

如果某接口应用了该策略，则不允许删除该策略，需要在应用的接口上取消对该策略的应用，然后再使用 **undo qos policy** 删除该策略。

2. 在策略中为类指定流行为

请在策略视图下进行下列配置。

表3-49 在策略中为类指定流行为

操作	命令
在策略中为类指定采用的流行为	classifier <i>tcl-name</i> behavior <i>behavior-name</i>
取消指定类在策略中的使用	undo classifier <i>tcl-name</i>

tcl-name: 类名，必须是已经定义的类，可以是系统定义或用户定义类。

behavior-name: 必须是已定义的流行为名，可以是系统定义或用户定义流行为。

3.6.5 应用策略

qos apply policy 命令是将一个策略映射到具体的接口上。一个策略映射可以在多个接口上得到应用。

请在接口视图或 ATM PVC 视图下进行下列配置。

表3-50 将接口或 ATM PVC 与所设置的策略相关联

操作	命令
在接口上应用关联的策略	qos apply policy <i>policy-name</i> { inbound outbound [dynamic] }
在接口上删除关联的策略	undo qos apply policy { inbound outbound }

dynamic 表示动态应用策略，只应用在拨号接口或 VT 接口配置了 MP 的情况下。当把 QoS 策略配置到拨号或 VT 接口上时，由于配置时可用带宽未必满足策略需要，应先用 **qos max-bandwidth** 命令在接口上配置足够的带宽，这样可保证策略配置到接口上。

QoS 策略在接口视图（除 ATM 接口）下应用的规格如下：

- | 封装 X.25 和 LAPB 的接口不能应用 CBQ。
- | 普通物理接口和 MP 引用的 VT, 可以应用配置了各种特性(包括 **remark**、**car**、**gts**、**queue af**、**queue ef**、**queue wfq**、**wred** 等)的策略。
- | 配置了流量整形 (**gts**) 和队列 (**queue ef**、**queue af**、**queue wfq**) 特性的策略, 不能作为入方向策略应用在入接口上。
- | 子接口不支持队列 (**queue ef**、**queue af**、**queue wfq**) 特性, 但是支持流量整形 (**gts**) 与流量监管 (**car**)。所以只配置了流量整形与流量监管的策略可以应用到子接口。

QoS 策略在 ATM 接口下应用比较特殊, 其规格如下:

- | 在入方向的 QoS 策略特性只能为 REMARK DSCP 或 REMARK IP-PRECEDENCE; 在出方向的 QoS 策略特性可以为 REMARK DSCP、REMARK IP-PRECEDENCE、REMARK ATMCLP、EF、AF、WFQ、CBQ。
- | 在 ATM PVC 接口下配置的 REMARK DSCP、REMARK IP-PRECEDENCE、CBQ 等策略只对 IPoA 协议有效, 对 IPoEoA、PPPoA、PPPoEoA 等都无效; 如果策略特性为 REMARK ATMCLP, 则对 IPoA、IPoEoA、PPPoA、PPPoEoA 等都有效。
- | 若对 IPoEoA、PPPoA、PPPoEoA 等协议报文应用 REMARK DSCP、REMARK IP-PRECEDENCE, 应通过在 VT 或 VE 接口上应用 QoS 策略来实现 (如果将这些策略应用在 ATM 物理接口上, 策略将不会起作用)。

3.6.6 基于类的队列的显示和调试

在完成上述配置后, 在所有视图下执行 **display** 命令可以显示基于类的队列的运行情况, 通过查看显示信息验证配置的效果。

表3-51 基于类的队列的显示和调试

操作	命令
显示路由器配置的类信息	display traffic classifier { system-defined user-defined } [<i>tcl-name</i>]
显示路由器配置的流行为信息	display traffic behavior { system-defined user-defined } [<i>behavior-name</i>]
显示指定策略中指定类及与类关联的流行为的配置信息	display qos policy { system-defined user-defined } [<i>policy-name</i> [classifier <i>tcl-name</i>]]
显示指定接口、指定 ATM 接口的指定 PVC 或所有接口与 PVC 上策略的配置信息和运行情况	display qos policy interface [<i>interface-type</i> <i>interface-number</i> [inbound outbound] [pvc { <i>pvc-name</i> [<i>vpi/vci</i>] <i>vpi/vci</i> }]]

操作	命令
显示指定接口、指定 ATM 接口的指定 PVC 或所有接口与 PVC 的基于类的队列配置信息和运行情况。	display qos cbq interface [<i>interface-type</i> <i>interface-number</i> [pvc { <i>pvc-name</i> [<i>vpi/vci</i>] <i>vpi/vci</i> }]]
显示队列调试信息	debugging qos cbq { ef af be }

3.7 RTP 优先队列的配置

RTP 报文队列的配置包括：

- | 在接口上应用 RTP 队列
- | 配置带宽限制
- | RTP 队列的显示和调试

3.7.1 在接口上应用 RTP 队列

设置接口上应用 RTP 队列。此命令没有缺省配置。

请在接口视图下进行如下配置。

表3-52 在接口上应用 RTP 队列

操作	命令
在接口上应用 RTP 队列	qos rtpq start-port <i>first-rtp-port-number</i> end-port <i>last-rtp-port-number</i> bandwidth <i>bandwidth</i> [cbs <i>committed-burst-size</i>]
关闭 RTP 队列在接口上的应用	undo qos rtpq



注意：

除链路层使用 X.25 及 LAPB 的接口外，所有物理接口都可以应用 RTP 队列。

3.7.2 配置最大预留带宽

配置最大预留带宽占接口实际可用带宽的百分比。

请在接口视图下进行下列配置。

表3-53 配置带宽限制

操作	命令
配置带宽限制	qos reserved-bandwidth pct <i>percentage</i>
恢复缺省的带宽限制	undo qos reserved-bandwidth

参数 *percentage* 是预留带宽占可用带宽的百分比，取值范围为 1~100，缺省值为 80。

3.7.3 RTP 报文队列的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示当前 RTP 队列机制的队列信息，包括当前的 RTP 队列长度和 RTP 报文的丢包数，显示所有接口的 RTP 队列配置情况和统计信息，通过查看显示信息验证配置的效果。

表3-54 显示接口 RTP 队列的配置情况和统计信息

操作	命令
显示接口 RTP 队列的配置情况和统计信息	display qos rtpq interface [<i>interface-type</i> / <i>interface-number</i>]

3.7.4 QoS 令牌功能

当进行 FTP 等数据传输工作时，如果配置了 QoS 的 CQ 和 WFQ，由于上层协议（如 TCP）提供了流控功能，可能会导致 QoS 的队列失效。VRP 提供了 QoS 令牌功能来解决这种问题。QoS 的发送令牌功能提供了一种底层队列的流量控制机制，它可以根据令牌的数量控制向底层接口队列发送的报文数量。

通常，在进行 FTP 传输时，建议将接口的发送令牌数量设置为 1。

如果上层协议（如 UDP）没有流控功能，建议不要使用 QoS 令牌功能，以提高数据传输的效率。

请在接口视图下进行下列配置。

表3-55 配置 QoS 令牌功能

操作	命令
配置 QoS 令牌功能	qmtoken <i>token-number</i>
取消 QoS 令牌功能	undo qmtoken

缺省情况下，未启用 QoS 令牌功能。

& 说明:

在配置了此命令后, 需要用 **shutdown / undo shutdown** 功能将接口重新启动, 才能使能 QoS 的发送令牌功能。

目前只有以太网接口、串口、BRI 接口支持该命令。

3.8 典型配置举例

3.8.1 优先队列配置举例

1. 配置需求

如图所示, Server 和 PC1 通过路由器 Quidway1 向 PC2 发送数据 (其中 Server 发送关键业务数据, PC1 发送非关键业务数据) 时, 由于 Quidway1 入接口 ethernet0/0/0 的速率大于出接口 serial2/0/0 的速率, 在 serial2/0/0 接口处可能发生拥塞, 导致丢包。要求在网络拥塞时保证 Server 发送的关键业务数据得到优先处理。

2. 组网图

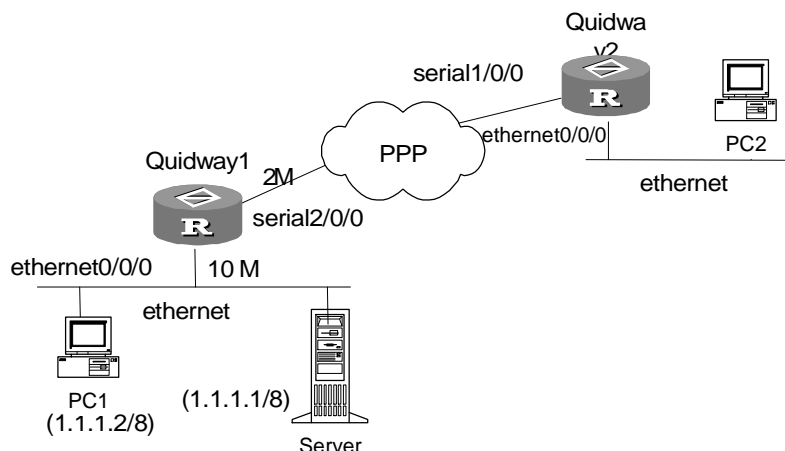


图3-6 优先队列配置组网图

3. 配置步骤

配置路由器 Quidway1:

配置 ACL 规则列表, 分别匹配来源于 Server 和 PC1 的报文。

```
[Quidway1] acl number 2001
[Quidway1-acl-basic-2001] rule permit source 1.1.1.1 0.0.0.0
[Quidway1] acl number 2002
[Quidway1-acl-basic-2002] rule permit source 1.1.1.2 0.0.0.0
```

配置优先队列规则组, 使得网络拥塞发生时, 源自 **Server** 的报文能够进入 PQ 的 **top** 队列缓存, 源自 **PC1** 的报文能够进入 **bottom** 队列缓存, 并且设定 **top** 队列的最大队列长度为 50、**bottom** 队列的最大队列长度为 100。

```
[Quidway1] qos pq1 1 protocol ip acl 2001 queue top
[Quidway1] qos pq1 1 protocol ip acl 2002 queue bottom
[Quidway1] qos pq1 1 queue top queue-length 50
[Quidway1] qos pq1 1 queue bottom queue-length 100
```

在接口 **serial2/0/0** 上启用优先队列规则组 1

```
[Quidway1] interface serial2/0/0
[Quidway1-Serial2/0/0] qos pq pq1 1
```

3.8.2 基于类的队列配置举例

1. 组网需求

在下面的组网图中, 从 **RouterC** 发出的数据流经过 **RouterA** 和 **RouterB** 到达 **RouterD**。**RouterC** 发出的数据流根据 IP 报文的 **DSCP** 域分为 4 类, 要求配置 QoS 策略, 对于 **DSCP** 域为 **AF11** 和 **AF21** 的流进行确保转发 (**AF**), 最小带宽为 5%; 对于 **DSCP** 域为 **EF** 的流进行加速转发 (**EF**), 最大带宽为 30%。

EF 流可以保证一定带宽, 并保证时延和时延抖动, 对于 **EF** 流的优先保证是通过 **LLQ** 技术实现的。**AF** 流只保证带宽, **DF** 流则没有带宽和时延保证。

在开始下面的配置之前, 应保证:

- 1 RouterC 发出的流能够通过 RouterA 和 RouterB 到达 RouterD。
- 1 报文的 **DSCP** 域在进入 RouterA 之前已经设置完毕。

2. 组网图

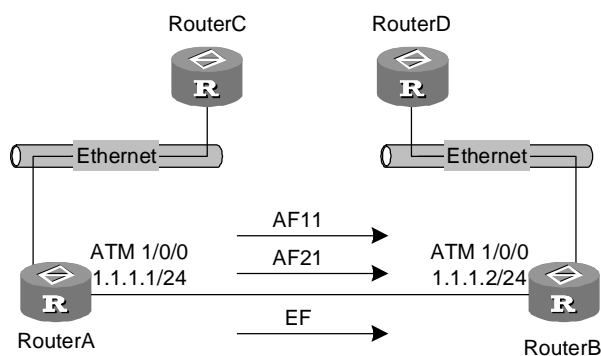


图3-7 基于类的队列配置组网图

3. 配置步骤

在 **RouterA** 上进行配置。

定义三个类，分别匹配 DSCP 域为 AF11、AF21 和 EF 的 IP 报文。

```
[Quidway] traffic classifier af11_class
[Quidway-classifier-af11_class] if-match dscp af11
[Quidway-classifier-af11_class] traffic classifier af21_class
[Quidway-classifier-af21] if-match dscp af21
[Quidway-classifier-af21] traffic classifier ef_class
[Quidway-classifier-ef_class] if-match dscp ef
[Quidway-classifier-ef_class] quit
```

定义流行为，配置 AF，并分配最小可用带宽。

```
[Quidway] traffic behavior af11_behav
[Quidway-behavior-af11_behav] queue af bandwidth pct 5
[Quidway-behavior-af11_behav] traffic behavior af21_behav
[Quidway-behavior-af21_behav] queue af bandwidth pct 5
[Quidway-behavior-af21_behav] quit
```

定义流行为，配置 EF，并分配最小可用带宽（对于 EF 流，将同时保证带宽和时延）。

```
[Quidway] traffic behavior ef_behav
[Quidway-behavior-ef_behav] queue ef bandwidth pct 30
[Quidway-behavior-ef_behav] quit
```

定义 QoS 策略，将已配置的流行为指定给不同的类。

```
[Quidway] qos policy dscp
[Quidway-qospolicy-dscp] classifier af11_class behavior af11_behav
[Quidway-qospolicy-dscp] classifier af21_class behavior af21_behav
[Quidway-qospolicy-dscp] classifier ef_class behavior ef_behav
[Quidway-qospolicy-dscp] quit
```

将已定义的 QoS 策略应用在路由器 RouterA 的 ATM PVC 出方向。

```
[Quidway] interface atm 1/0/0
[Quidway-atm1/0/0] ip address 1.1.1.1 255.255.255.0
[Quidway-atm1/0/0] pvc qostest 0/40
[Quidway-atm-pvc-atm1/0/0-0/40-qostest] qos apply policy dscp outbound
```

配置完成后，当发生拥塞时，可以观察到 EF 流被以较高的优先级转发。

3.8.3 定制队列配置举例

1. 组网需求

在下面的组网图中，两台路由器 RouterA 和 RouterB 通过一条 PPP 链路背靠背连接，连接 RouterA 的 PC 机作为 FTP 以及 HTTP 的服务器端，连接 RouterB 的 PC 机作为 FTP 以及 HTTP 的客户端。配置路由使得数据流均经过 RouterA 的接口转发至 RouterB。

在开始下列配置前应保证：

- 1 RouterA 与 RouterB 建立起 PPP 连接，并且两台 PC 机建立起 FTP 连接。
- 1 连接 RouterB 的 pc 机作为客户端从连接 RouterA 的 server 端下载一个较大的文件，同时用 RouterB 端的 pc 机用 http 协议从 RouterA 端的 http server 上下载大文件。

定制 FTP 数据流与 HTTP 数据流以 1:2 的比例分享链路带宽。

2. 组网图

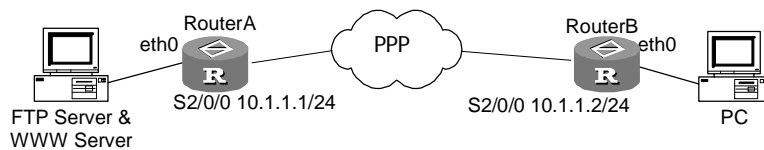


图3-8 定制队列配置组网图

3. 配置步骤

在 RouterA 上进行配置。

配置 acl 规则分别匹配 FTP 报文与 HTTP 报文：

```
[Quidway] acl number 3001
[Quidway-acl-adv-3001] rule 0 permit tcp source-port eq ftp
[Quidway-acl-adv-3001] rule 1 permit tcp source-port eq ftp-data
[Quidway-acl-adv-3001] rule 2 deny ip
[Quidway] quit
[Quidway] acl number 3002
[Quidway-acl-adv-3001] rule 0 permit tcp source-port eq www
[Quidway-acl-adv-3001] rule 1 deny ip
[Quidway-acl-adv-3001] quit
```

配置 CQ 规则，定制 FTP 流与 HTTP 流按 1：2 的比例分享链路带宽。

```
[Quidway] qos cql 1 queue 11 serving 1000
[Quidway] qos cql 1 queue 12 serving 2000
[Quidway] qos cql 1 protocol ip acl 3001 queue 11
[Quidway] qos cql 1 protocol ip acl 3002 queue 12
```

将该规则应用在接口的出方向上。

```
[Quidway] interface Serial2/0/0
[Quidway1-Serial2/0/0] link-protocol ppp
[Quidway1-Serial2/0/0] ip address 10.1.1.1 255.255.255.0
[Quidway1-Serial2/0/0] qos cq cql 1
[Quidway1-Serial2/0/0] quit
```

3.8.4 CBQ 基于类的队列配置举例

1. 组网需求

在下面的组网图中，两台路由器 RouterA 和 RouterB 上都配置 FXS 卡，并连接电话。两台路由器背靠背连接并封装 PPP。两台路由器配置 VOIP，使得语音报文经过 RouterA 的 Serial 2/0/0 接口转发至 RouterB。连接 RouterB 的 pc 机作为客户端，连接 RouterA 的 pc 机作为 FTP 与 WWW 的服务器端。

- l 作为客户端的 PC 机从连接 RouterA 的 Server 上同时用 FTP 方式与 HTTP 方式下载较大的文件。
- l 从 RouterA 向 RouterB 拨通一路电话。

预期达到的效果：

- l 在链路拥塞的状况下，通话质量应该不受其他流量的影响。
- l 从客户端观察下载速率，两种方式的下载速率成比例关系。比例大小为分别配置的最小可占用带宽的比例。HTTP 与 FTP 的比例为 1：2。
- l FTP 的传输速率不小于 64Kbps，HTTP 的传输速率不小于 32Kbps。

2. 组网图

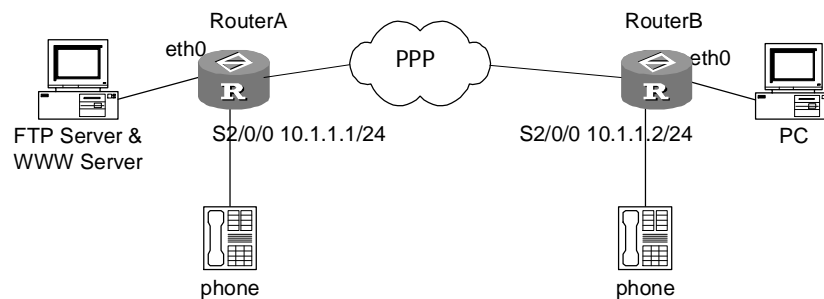


图3-9 CBQ 基于类的队列配置组网图

3. 配置步骤

(1) 配置在 RouterA

配置 VOIP

```

[Quidway] voice-setup
[Quidway-voice] dial-program
[Quidway-voice-dial] entity 2631 pots
[Quidway-voice-dial-entity2631] match-template 2631
[Quidway-voice-dial-entity2631] line 0
[Quidway-voice-dial-entity2631] quit
[Quidway-voice-dial] entity 3680 voip
[Quidway-voice-dial-entity3680] address ip 10.1.1.2
[Quidway-voice-dial-entity3680] match-template 3680
  
```

配置 acl 规则分别匹配 FTP、HTTP 报文以及语音报文。

```
[Quidway] acl number 3001 match-order auto
[Quidway-acl-adv-3001] rule 0 permit tcp source any source-port eq ftp
destination any
[Quidway-acl-adv-3001] rule 1 permit tcp source any source-port eq ftp-data
destination any
[Quidway-acl-adv-3001] rule 2 deny ip source any destination any
[Quidway-acl-adv-3001] quit
[Quidway] acl number 3002 match-order auto
[Quidway-acl-adv-3002] rule 0 permit tcp source any source-port eq www
destination any
[Quidway-acl-adv-3002] rule 1 deny ip source any destination any
[Quidway-acl-adv-3002] quit
[Quidway] acl number 3011 match-order auto
[Quidway-acl-adv-3011] rule 0 permit udp source any source-port range 16384
32768 destination any destination-port range 16384 32768
[Quidway-acl-adv-3011] quit
```

配置 classifier 匹配 acl 规则。

```
[Quidway] traffic classifier ftp operator and
[Quidway-classifier-ftp] if-match acl 3001
[Quidway-classifier-ftp] quit
[Quidway] traffic classifier http operator and
[Quidway-classifier-http] if-match acl 3002
[Quidway-classifier-http] quit
[Quidway] traffic classifier voice operator and
[Quidway-classifier-voice] if-match acl 3011
[Quidway-classifier-voice] quit
```

配置 behavior。

```
[Quidway] traffic behavior ftp
[Quidway-behavior-ftp] queue af bandwidth 64
[Quidway-behavior-ftp] quit
[Quidway] traffic behavior http
[Quidway-behavior-http] queue af bandwidth 32
[Quidway-behavior-http] quit
[Quidway] traffic behavior voice
[Quidway-behavior-voice] queue ef bandwidth 32 cbs 1500
[Quidway-behavior-voice] quit
```

配置 policy，将对应的 classifier 和 behavior 关联，语音报文进入 EF 队列优先发送，并配置匹配 ftp 类与 http 类的报文均进入 AF 队列

```
[Quidway] qos policy CBQ
```

```
[Quidway-qospolicy-CBQ] classifier ftp behavior ftp
[Quidway-qospolicy-CBQ] classifier http behavior http
[Quidway-qospolicy-CBQ] classifier voice behavior voice
[Quidway-qospolicy-CBQ] quit
```

FTP 报文进入 AF 队列，保证最小可占用带宽为 64K；HTTP 报文进入 AF 队列，保证最小可占用带宽为 32K；语音报文进入 EF 队列优先发送，最大占用带宽为 32K。

将该规则应用在接口的出方向上

```
[Quidway] interface Serial2/0/0
[Quidway-Serial2/0/0] link-protocol ppp
[Quidway-Serial2/0/0] ip address 10.1.1.1 255.255.255.0
[Quidway-Serial2/0/0] qos max-bandwidth 2048
[Quidway-Serial2/0/0] qos apply policy CBQ outbound
```

3.8.5 Qos 策略嵌套及 LR 综合应用配置举例

1. 组网需求

如下图所示，假设 PC1 通过路由器 Quidway1 向 PC2 发送关键业务数据，同时，路由器 Quidway1 作为 hwping 的客户端向作为 hwping 的服务器端的路由器 Quidway2 发送网络性能监测数据。由于 Quidway1 入接口 ethernet1/0/0 的速率（10M）大于出接口 serial3/0/0 的速率，在 serial3/0/0 接口处可能发生拥塞（串口速率为 2Mbps），导致丢包。现在希望在网络拥塞时，对关键业务数据和网络性能监测数据共同保证 256K 的带宽；限制关键业务数据的流量不超过 CIR——262K，但是不希望超出的流量直接被抛弃；同时，为了保证网络性能监测数据的流量能够畅通无阻，所以不希望限速作用于网络性能监测数据流量。这就需要，一方面将关键业务数据和网络性能监测数据配置到一个类中，入同一个 AF 队列；另一方面将非网络性能监测数据划分出来，单独进行流量限速。

2. 组网图

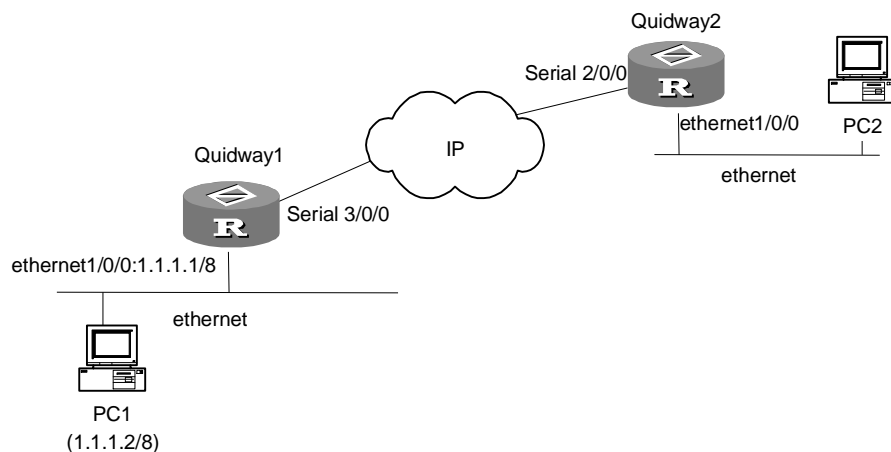


图3-10 Qos 策略嵌套组网图

3. 配置步骤

(1) 配置路由器 Quidway1

配置 ACL 规则列表，分别匹配关键业务数据报文和网络性能监测数据报文。

```
[Quidway1] acl number 2002
[Quidway1-acl-basic-2002] rule permit source 1.1.1.2 0.0.0.0
[Quidway1-acl-basic-2002] acl number 2001
[Quidway1-acl-basic-2001] rule permit source 1.1.1.1 0.0.0.0
[Quidway1-acl-basic-2001] quit
```

配置关键业务数据类和网络性能监测数据类。

```
[Quidway1] traffic classifier Critical
[Quidway1-classifier-Critical] if-match acl 2002
[Quidway1-classifier-Critical] traffic classifier Crit&Hwping
[Quidway1-classifier-Crit&Hwping] if-match acl 2001
[Quidway1-classifier-Crit&Hwping] if-match acl 2002
```

配置应用于关键业务数据类和网络性能监测数据类的 AF 队列行为。

```
[Quidway1-classifier-Crit&Hwping] traffic behavior AF
[Quidway1-behavior-AF] queue af bandwidth 256
```

配置应用于关键业务数据类的 LR 行为。

```
[Quidway1-behavior-AF] traffic behavior LR
[Quidway1-behavior-LR] lr cir 262000 cbs 262000 ebs 0
```

配置子策略，为网络性能监测数据数据类应用 LR。

```
[Quidway1-behavior-CAR] qos policy Child
[Quidway1-trafficpolicy-Child] classifier Crit&Hwping behavior LR
```

配置父策略，为关键业务数据类和网络性能监测数据类应用 AF 队列行为。

```
[Quidway1-trafficpolicy-Child] qos policy Parent
[Quidway1-trafficpolicy-Parent] classifier Crit&Hwping behavior AF
```

配置策略嵌套，在父策略下应用子策略。

```
[Quidway1-trafficpolicy-Parent] traffic behavior AF
[Quidway1-behavior-AF] traffic-policy Child
```

在接口上应用父策略。

```
[Quidway1-Serial3/0/0] qos apply policy Parent outbound
```

3.8.6 ATM PVC Remark 策略典型配置举例

1. 组网需求

如下图所示，三台路由器 A、B 和 C 接入到 ATM 网中互相通讯，要求：

- l 三台路由器 ATM 接口的 IP 地址分别是 202.38.160.1、202.38.160.2、202.38.160.3;
- l 在 ATM 网中, 路由器 A 的 VPI/VCI 是 0/40 和 0/41, 分别连接路由器 B 和路由器 C; 路由器 B 的 VPI/VCI 是 0/50 和 0/51, 分别连接路由器 A 和路由器 C; 路由器 C 的 VPI/VCI 是 0/60 和 0/61, 分别连接路由器 A 和路由器 B;
- l 三台路由器的 ATM 接口上的所有 PVC 都采用 IPoA 应用方式。
- l 在路由器 A 出接口上配置 remark dscp 策略。

2. 组网图

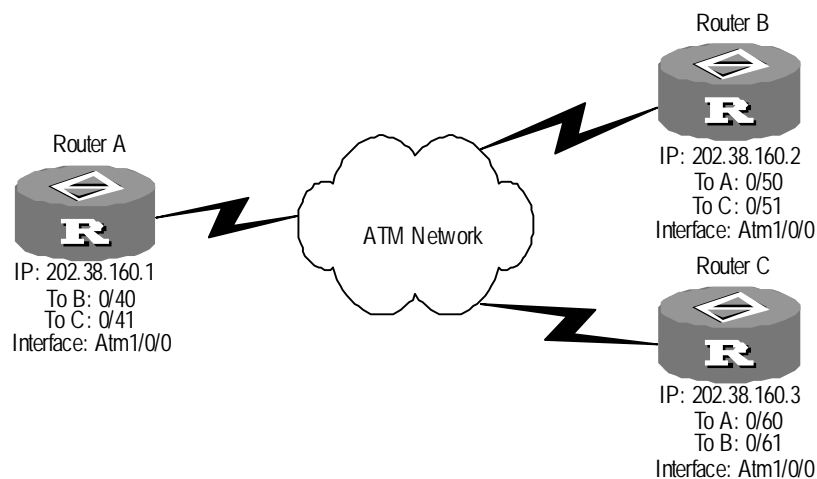


图3-11 ATM PVC Remark 策略典型配置举例

3. 配置步骤

(1) 配置路由器 A

进入 ATM 接口 (如图所示为 atm1/0/0), 并为其配置 IP 地址。

```
<Quidway> system-view
[Quidway] interface atm 1/0/0
[Quidway-atm1/0/0] ip address 202.38.160.1 255.255.255.0
```

创建 PVC, 并指定承载 IP 协议。

```
[Quidway-atm1/0/0] pvc to_b 0/40
[Quidway-atm-pvc-atm1/0/0-0/40-to_b] map ip 202.38.160.2
[Quidway-atm-pvc-atm1/0/0-0/40-to_b] quit
[Quidway-atm1/0/0] pvc to_c 0/41
[Quidway-atm-pvc-atm1/0/0-0/41-to_c] map ip 202.38.160.3
[Quidway-atm-pvc-atm1/0/0-0/41-to_c] quit
[Quidway-atm1/0/0] quit
```

配置 classifier 1 的匹配条件。

```
[Quidway] traffic classifier 1
[Quidway-classifier-1] if-match ip-precedence 3

# 配置 behavior 1 的行为。

[Quidway-classifier-1] traffic behavior 1
[Quidway-behavior-1] remark dscp af31

# 配置策略 policy 1。

[Quidway] qos policy 1
[Quidway-qospolicy-1] classifier 1 behavior 1
[Quidway-qospolicy-1] quit

# 在 ATM PVC 出方向上应用策略 policy 1。

[Quidway] interface atm 1/0/0
[Quidway-atm1/0/0] pvc to_b 0/40
[Quidway-atm-pvc-atm1/0/0-0/60-to_a] qos apply policy 1 outbound
```

(2) 配置路由器 B

进入 ATM 接口（如图所示也为 atm1/0/0），并为其配置 IP 地址。

```
<Quidway> system-view
[Quidway] interface atm 1/0/0
[Quidway-atm1/0/0] ip address 202.38.160.2 255.255.255.0
```

创建 PVC，并指定承载 IP 协议。

```
[Quidway-atm1/0/0] pvc to_a 0/50
[Quidway-atm-pvc-atm1/0/0-0/50-to_a] map ip 202.38.160.1
[Quidway-atm-pvc-atm1/0/0-0/50-to_a] quit
[Quidway-atm1/0/0] pvc to_c 0/51
[Quidway-atm-pvc-atm1/0/0-0/51-to_c] map ip 202.38.160.3
```

(3) 配置路由器 C

进入 ATM 接口（如图所示也为 atm1/0/0），并为其配置 IP 地址。

```
<Quidway> system-view
[Quidway] interface atm 1/0/0
[Quidway-atm1/0/0] ip address 202.38.160.3 255.255.255.0
```

创建 PVC，并指定承载 IP 协议。

```
[Quidway-atm1/0/0] pvc to_a 0/60
[Quidway-atm-pvc-atm1/0/0-0/60-to_a] map ip 202.38.160.1
[Quidway-atm-pvc-atm1/0/0-0/60-to_a] quit
[Quidway-atm1/0/0] pvc to_b 0/61
[Quidway-atm-pvc-atm1/0/0-0/61-to_b] map ip 202.38.160.2
```

RouterA 在出接口上修改了报文的 dscp 值，后续路由器可以根据收到报文的 dscp 值对报文做一些相关处理，比如：过滤掉某些优先级的报文，让某些优先级的报文

先发送（即发送的优先级高）或限制某些优先级报文所占用的最大带宽等等，其配置方法这里不再具体说明。

第4章 拥塞避免

4.1 拥塞避免简介

过度的拥塞会对网络资源造成极大危害，必须采取某种措施加以解除。这里所说的拥塞避免（Congestion Avoidance），是指通过监视网络资源（如队列或内存缓冲区）的使用情况，在拥塞有加剧的趋势时，主动丢弃报文，通过调整网络的流量来解除网络过载的一种流控机制。

与端到端的流控相比，这里的流控有更广泛的意义，它影响到路由器中更多的业务流的负载。当然，路由器在丢弃报文时，并不排斥与源端的流控动作比如 TCP 流控的配合，更好地调整网络的流量到一个合理的负载状态。好的丢包策略和源端流控机制的组合，总是追求网络的吞吐量和利用效率最大化，并且使报文丢弃和延迟最小化。

1. 传统的丢包策略

传统的丢包策略采用尾部丢弃（Tail-Drop）的方法。当队列的长度达到某一最大值后，所有新到来的报文都将被丢弃。

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

2. RED 与 WRED

为避免 TCP 全局同步现象，可使用 RED（Random Early Detection，随机早期检测）或 WRED（Weighted Random Early Detection，加权随机早期检测）。

在 RED 类算法中，为每个队列都设定一对低限和高限值，并规定：

- 1 当队列的长度小于低限时，不丢弃报文。
- 1 当队列的长度超过高限时，丢弃所有到来的报文。
- 1 当队列的长度在低限和高限之间时，开始随机丢弃到来的报文。方法是为每个到来的报文赋予一随机数，并用该随机数与当前队列的丢弃概率比较，如果大于丢弃概率则被丢弃。队列越长，丢弃概率越高——但有一个最大丢弃概率。

与 RED 不同，WRED 生成的随机数是基于优先权的，它引入 IP 优先权区别丢弃策略，考虑了高优先权报文的利益并使其被丢弃的概率相对较小。

RED 和 WRED 通过随机丢弃报文避免了 TCP 的全局同步现象——当某个 TCP 连接的报文被丢弃，开始减速发送的时候，其他的 TCP 连接仍然有较高的发送速度。这样，无论什么时候，总有 TCP 连接在进行较快的发送，提高了线路带宽的利用率。

直接采用队列的长度和低限、高限比较并进行丢弃(这是设置队列门限的绝对长度),将会对突发性的数据流造成不公正的待遇,不利于数据流的传输。所以,在和低限、高限比较并进行丢弃时,采用队列的平均长度(这是设置队列门限与平均长度比较的相对值)。队列的平均长度是队列长度被低通滤波后的结果。它既反映了队列的变化趋势,又对队列长度的突发变化不敏感,避免了对突发性数据流的不公正待遇。

当队列机制采用 WFQ 时,可以为不同优先级 (precedence) 的报文设定不同的队列长度滤波系数、上限、下限、丢弃概率,从而对不同优先级的报文提供不同的丢弃特性。

当队列机制采用 FIFO、PQ、CQ 时,可以为每个队列设定不同的队列长度滤波系数、低限、高限、丢弃概率,为不同类别的报文提供不同的丢弃特性。

WRED 和队列机制的关系如下图所示。

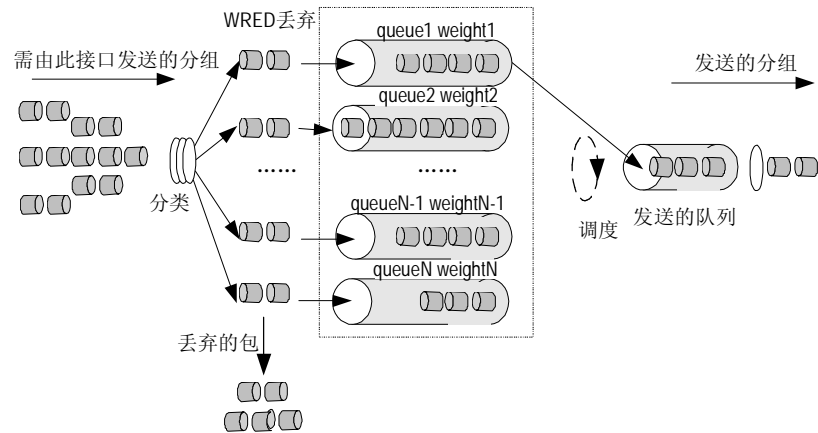


图4-1 WRED 和队列机制关系示意图

当 WRED 和 WFQ 配合使用时,可以实现基于流的 WRED。这是因为,在进行分类的时候,不同的流有自己的队列,对于流量小的流,由于其队列长度总是比较小,所以丢弃的概率将比较小。而流量大的流将会有较大的队列长度,从而丢弃较多的报文,保护了流量较小的流的利益。

4.2 WRED 的配置

WRED 的配置包括:

- l 使用 WRED
- l 设置 WRED 计算平均队列长度的指数
- l 设置 WRED 各优先级参数

4.2.1 使用 WRED

请在接口视图下进行下列配置。

表4-1 使用 WRED

操作	命令
使用 WRED	qos wred
恢复缺省形式	undo qos wred

WRED 只能和 WFQ 共同使用，不能单独使用或和其它的队列共同使用。

缺省情况为不使用 WRED，队列的丢弃方法为尾部丢弃。

& 说明：

使用 WRED 之前接口上必须已经应用了 WFQ。

4.2.2 设置 WRED 计算平均队列长度的指数

设置 WRED 计算平均队列长度的滤波系数。

请在接口视图下进行下列配置。

表4-2 设置 WRED 计算平均队列长度的指数

操作	命令
设置 WRED 计算平均队列长度的指数	qos wred weighting-constant <i>exponent</i>
恢复指数的缺省值	undo qos wred weighting-constant

其中 *exponent* 为计算平均队列长度的滤波系数，取值范围为 1~16，缺省值为 9。

必须先使用 **qos wred** 在接口上应用 WRED，才可以配置 WRED 的参数。

4.2.3 设置 WRED 各优先级参数

当接口配置加权公平队列时，可以设置 WRED 各优先级的下限、上限以及丢弃概率分母。

请在接口视图下进行下列配置。

表4-3 设置 WRED 各优先级参数

操作	命令
设置 WRED 优先级参数	qos wred ip-precedence <i>ip-precedence low-limit low-limit high-limit high-limit discard-probability discard-prob</i>
恢复各优先级参数的缺省值	undo qos wred ip-precedence <i>ip-precedence</i>

必须先使用 **qos wred** 在接口上应用 WRED，才可以配置 WRED 的参数。

4.3 WRED 的显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示接口的 WRED 配置情况和统计信息，通过查看显示信息验证配置的效果。

表4-4 显示接口的 WRED 配置情况和统计信息

操作	命令
显示接口的 WRED 配置情况和统计信息	display qos wred interface [<i>interface-type</i> <i>interface-number</i>]

该命令可以显示某个接口或所有接口的 WRED 配置情况和统计信息

- | **interface-type** 为接口类型。
- | **interface-number** 为接口号。

第5章 帧中继 QoS

5.1 帧中继 QoS 简介

5.1.1 帧中继 QoS

在帧中继接口上，可以使用通用的 QoS 服务为用户提供接口上的流量监管、流量整形、拥塞管理、拥塞避免等服务。除此之外，帧中继网络还拥有自己的 QoS 服务机制，包括帧中继流量整形、帧中继流量监管、帧中继拥塞管理、帧中继 DE（Discard Eligibility）规则列表、帧中继队列管理等。利用这些功能，网络服务提供商可以根据不同的需求，为用户提供带宽限制、带宽预留等服务。

与通用的 QoS 相比，帧中继 QoS 能够在接口的每条虚电路上提供 QoS 服务，而通用 QoS 只能在整个接口上提供 QoS 服务。因此帧中继 QoS 能够为用户提供更灵活的质量服务。

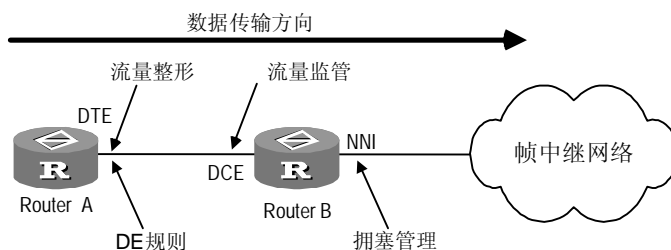


图5-1 帧中继 QoS 应用示意图

5.1.2 重要参数

下面列出了对 FR 进行控制的一些重要参数。

允许的承诺信息速率（CIR ALLOW）：FR 正常情况下可以提供的传送速率。网络不拥塞时，可以保证用户可以以此速率传送数据。

承诺信息速率（CIR）：虚电路可以提供的最小传送速率。即使网络拥塞，也可以保证用户可以以此速率传送数据。

承诺信息流量（CBS）：FR 网络承诺的在 Tc 时间内传送的包流量。在网络拥塞时，FR 网络保证这部分可以成功地传送。

突发信息流量（EBS）：在 Tc 时间内，FR 网络可以超过承诺信息流量的最大值。在网络拥塞时，这上部分流量将被首先丢弃。因此，FR 网络不保证这上部分流量能被成功地传送。

5.1.3 帧中继 OoS 的实现

帧中继流量整形能够限制从某一虚电路发出的报文流量和突发报文流量，使这类报文能够以比较均匀的速度向外发送。

1. 帧中继流量整形

帧中继流量整形能够限制从某一虚电路发出的报文流量和突发报文流量，使这类报文能够以比较均匀的速度向外发送。

在帧中继网络中，如果不同的网段带宽不匹配，往往会在网段的交界处产生瓶颈。如下图所示，如果路由器 B 以 128 Kbps 的速率向路由器 A 发送报文，而路由器 A 的接口速率最大只能达到 64 Kbps，这时就会在帧中继网络与路由器 A 的连接处产生瓶颈，从而发生拥塞，导致数据无法被正常传送。

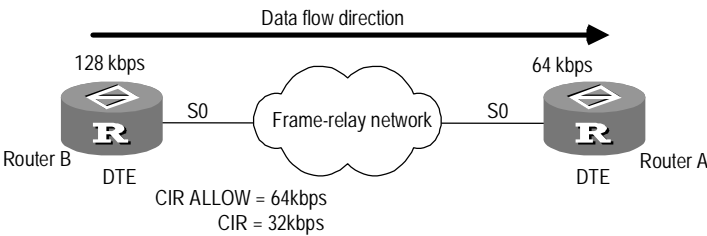


图5-2 帧中继流量整形示意图

因此，如果在路由器 B 的出接口 Serial 0 应用帧中继流量整形，可以使它以相对比较均匀的速率 64 Kbps 发送报文，从而避免网络拥塞的发生。即使网络发生拥塞，路由器 B 仍能够以 32 Kbps 的速率发送报文。

帧中继流量整形应用在路由器的输出接口，它可以向用户提供 CIR ALLOW（Committed Information Rate ALLOW，允许的承诺信息速率）、CIR（Committed Information Rate，承诺信息速率）、CBS（Committed Burst Size，承诺信息流量）、EBS（Excess Burst Size，突发信息流量）等参数。

帧中继虚电路能够以 CIR ALLOW 的速率发送报文。帧中继流量整形还允许虚电路在突发情况下以超过 CIR ALLOW 的速率发送报文。

帧中继流量整形是用令牌桶的算法实现的，根据实际的算法原理对协议中相关参数的含义进行了相应的修改。令牌桶原理如下图所示：

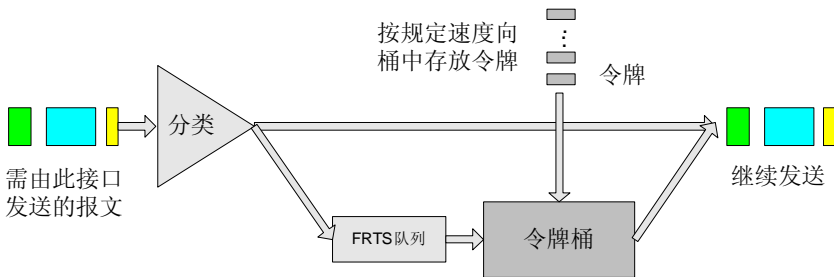


图5-3 FRTS 令牌桶原理

令牌桶原理是：需要进行流量控制的报文在发送前进入令牌桶中进行处理。如果令牌桶中有足够的令牌可以用来发送报文，则允许报文通过，即报文被正常发送。如果令牌桶中的令牌数不满足报文发送条件，则报文会放入 **FRTS** 队列，等令牌桶中有足够的令牌再从 **FRTS** 队列中取报文发送。这样，就可以对某类报文的流量进行控制。令牌的单位为 bit。

协议规定的相关参数和为华为 3COM 帧中继流量整形原理参数的对应关系如下：

CBS 和 **EBS** 的和为令牌桶大小，**CIR ALLOW** 为每秒向令牌桶中添加的令牌数。帧中继流量整形方案中为了提高效率，提出了动态 **Tc** 的概念。**Tc** 参数的大小在 10 到 100 毫秒之间，可根据每次发送的报文大小进行动态调节， $Tc = \text{size of packet} / CIR$ 。即无论待发送报文大小为多少（小于 1500 字节），路由器都会在当前计算出的 **Tc** 时间内，将所需要全部令牌分发给当前报文。

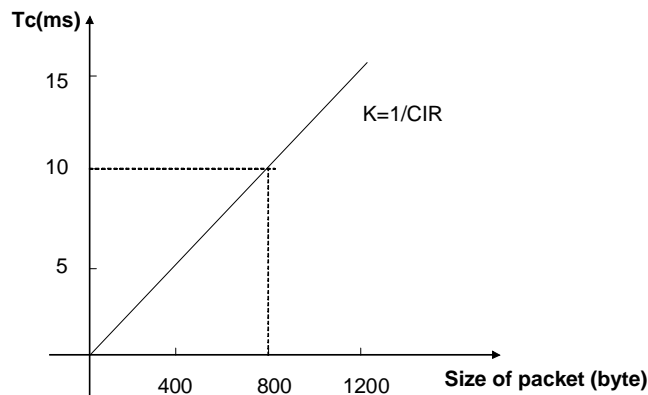


图5-4 Tc、CIR 关系示意图

如发送一个 800 字节的报文，需要 $800 \times 8 = 6400\text{bit}$ 的令牌。设 **CIR** 为 64000bps，则向令牌桶中添加发送该报文令牌需要的时间为 $6400 / 64000 = 0.1\text{s}$ （即 100ms），即对于该报文来说 **Tc** 为 100ms。100ms 之内令牌桶中添加了 6400bit 的令牌，该报文即被送出。特殊的，此时如果 **CIR** 为 8000bps，则该报文的令牌时间为 $6400 / 8000 = 800\text{ms} > 100\text{ms}$ ，但是由于 **Tc** 参数大小被定义在 10ms 到 100ms 之间滑动，此时 **Tc** 取其下限值为 100ms，而不是计算得到的 800ms。同样的，如果此时 **CIR** 为 1024000bps，则该报文的令牌时间为 $6400 / 1024000 = 6.25\text{ms} < 10\text{ms}$ ，但是由于 **Tc** 参数大小被定义在 10ms 到 100ms 之间滑动，所以该报文的 **Tc** 取其上限值 10ms。

由于 **CBS** 与 **EBS** 的和是令牌桶的大小，同时我司路由器是一次性分配令牌给待发送报文，为了使令牌桶中的令牌能够满足任何大小报文的发送，特别是大报文的发送，比如 1500byte 的报文，该报文发送需要 $1500 \times 8 = 12\text{Kbit}$ 的令牌。故我司路由器规定的 **CBS** 不得小于 15K，同时建议客户配置 **CBS** 的大小等同 **CIR** 的大小。

按照标准协议中规定，若 **Tc** = 20ms，**CIR** 为 64000bps，则每个 **Tc** 时间内只能添加 $0.02 \times 64000 = 1280\text{bit}$ 的令牌。如发送长度为 800 字节的报文需要 5 个 **Tc**，即

添加 5 次令牌才能将该报文发送出去。与标准协议的实现方式相比，我们在一个动态 Tc 中只需添加一次令牌就可将该报文发送出，大大提高了提高工作效率。

当网络发生拥塞时，如果帧中继交换侧配置了拥塞管理功能，它会通知路由器网络发生了拥塞。路由器接收到了网络拥塞的通知后，会使发送速率逐渐下降到 CIR，以缓解网络的拥塞状况，此时用户仍然能够以 CIR 的速率发送数据。此后如果路由器在一定时间内没有再收到网络拥塞的通知，发送速率又会逐渐由 CIR 上升回 CIR ALLOW。

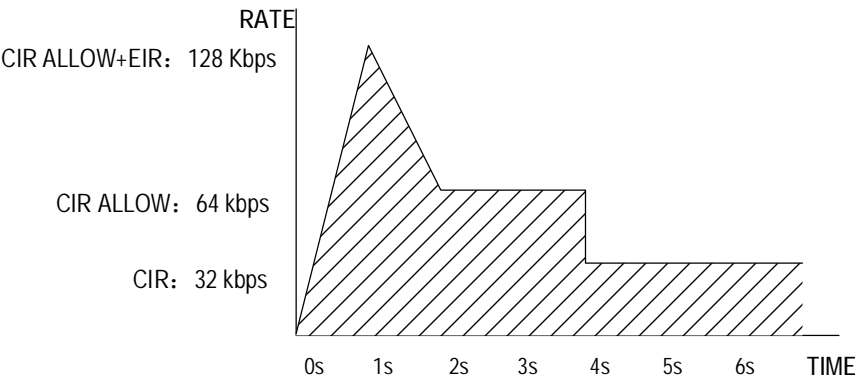


图5-5 帧中继流量整形原理示意图

如上图所示，设置帧中继流量整形参数分别为：CIR ALLOW=64 kbps，CIR=32 kbps，CBS=64000 bit，EBS=64000 bit，令牌桶的大小为 128000，在 4s 之前令牌桶添加令牌的速率为 64Kbps.，虚电路 64Kbps 的速率发送报文。当在 4s 时，路由器收到了带有 BECN 标志位的帧中继报文，表明网络发生拥塞，令牌桶添加令牌的速率下降为 CIR32Kbps,，虚电路以 32Kbps 的速率发送报文。

2. 帧中继流量监管

帧中继流量监管可以对每个虚电路上进入网络的流量进行监督，限制它在一个允许的范围之内。若某条虚电路的报文流量超过了用户设置的范围，则路由器会采取丢弃报文等措施，以保护网络资源和运营商的利益不受损害。

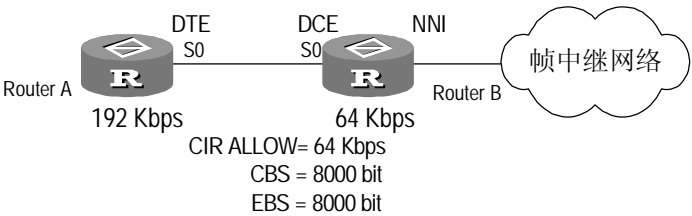


图5-6 帧中继流量监管示意图

如上图所示，用户端路由器 A 以 192 Kbps 的速率向交换端路由器 B 发送报文，但路由器 B 希望只为路由器 A 提供 64 Kbps 的带宽。这时就需要在路由器 B 的 DCE 端配置帧中继流量监管。

帧中继流量监管只能应用于路由器的 DCE 接口上，它可以对从 DTE 端发送来的报文流量进行监视。当报文流量小于 CBS 时，报文可以正常发送，路由器对报文不做处理；当流量大于 CBS 并小于 EBS 与 CBS 之和时，报文可以正常发送，但对于流量大于 CBS 的报文路由器将把帧中继报文头的中的 DE 标志位置为 1；当报文流量大于 CBS+EBS 时，路由器将以 CBS+EBS 的流量进行发送，对超过 CBS+EBS 的流量进行丢弃，对于超过 CBS 的流量 EBS，路由器将把帧中继报文头的中的 DE 标志位置为 1。

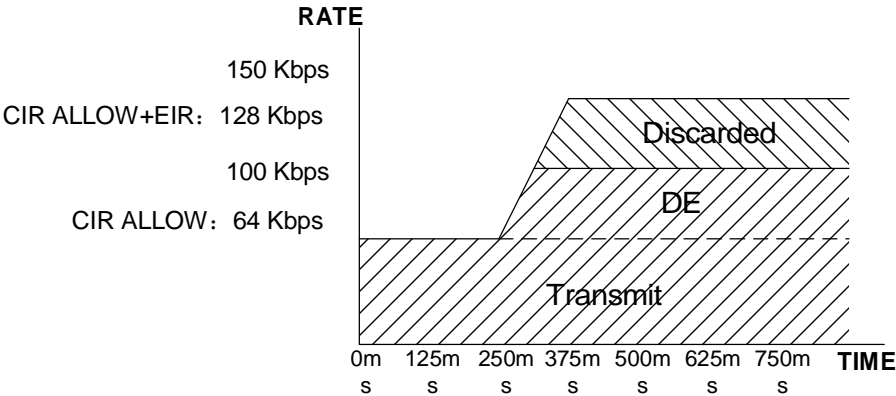


图5-7 帧中继流量监管原理示意图

如上图所示，设置帧中继流量监管参数分别为：CIR ALLOW=64 kbps，CBS=8000 bit，EBS=8000 bit，时间间隔 $T_c = CBS / CIR\ ALLOW = 125ms$ 。在 0~250ms 时，DTE 以速率 64 Kbps 向 DCE 发送报文，DCE 对这部分报文正常转发，转发的速率为 64 Kbps。在 250~500ms 时，DTE 以速率 100 Kbps 向 DCE 发送报文，DCE 的转发速率为 100 Kbps，但是超过 CBS 流量报文的 DE 标志位被置为 1。在 500ms 以后，DTE 以速率 150 Kbps 向 DCE 发送报文，DCE 的转发速率为 128 Kbps，超过 CBS 但小于 CBS+EBS 流量报文的 DE 标志位被置为 1，超过 CBS+EBS 流量的报文被直接丢弃。

3. 帧中继队列管理

除了帧中继虚电路队列之外，帧中继接口也拥有接口队列。当帧中继流量整形没有被使能的情况下，将只有帧中继接口队列起作用，也即预先配置的帧中继 PVC 队列只有在帧中继流量整形被使能的情况下才能生效。

虚电路队列和接口队列的关系如下图所示。

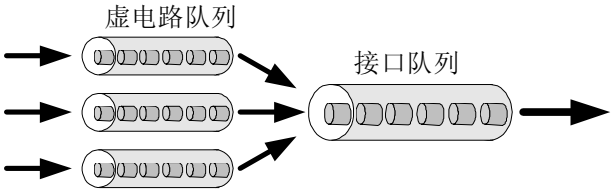


图5-8 帧中继队列示意图

在帧中继接口上能够使用的队列有：

- | FIFO: First-In First-Out Queueing, 先进先出队列
- | PQ: Priority Queueing, 优先队列
- | CQ: Custom Queueing, 定制队列
- | WFQ: Weighted Fair Queueing, 加权公平队列
- | CBQ: Class-Based Queueing, 基于类的队列
- | RTPQ: Realtime Transport Protocol Priority Queueing, 实时传输协议优先队列
- | PVC PQ: PVC Priority Queueing, 虚电路优先级队列

其中，FIFO、PQ、CQ、WFQ、CBQ 和 RTPQ 队列属于通用的队列，关于它们的详细介绍请参考《VRP3.4 操作手册 QoS》部分。

PVC PQ 队列被应用于帧中继接口之上，它拥有四种队列类型：top、middle、normal、bottom，队列优先级依次降低。同一虚电路发送的报文只能入 PVC PQ 中的一种队列，不同虚电路上的报文根据虚电路所处的优先级入接口下的 PVC PQ 队列。PVC PQ 的队列发送策略是：按照队列优先级，在优先级高的队列发送完毕后，再发送低优先级队列中的报文。

帧中继虚电路的队列包括：FIFO, PQ, CQ, WFQ, CBQ and RTPQ。RTPQ 可以与其它队列共存，而其它队列不能共存。

当接口实行帧中继流量整形时，队列类型只能是：FIFO、RTPQ 或 PVC PQ。

4. 帧中继拥塞管理

帧中继拥塞管理可以在网络发生拥塞时对帧中继报文进行处理：丢弃 DE 标志位为 1 的报文；同时发送拥塞通知至网络上的其他设备，告知其发生了拥塞。

帧中继拥塞管理应用于帧中继交换设备的出接口上。当拥塞没有发生时，对于转发的帧中继报文，路由器将正常转发，不作特殊处理。当拥塞发生时，DE 标志位为 1 的报文将会被丢弃；对于转发的正向报文，路由器把帧中继报文头的 FECN 标志位置为 1；对于同一虚电路上反方向发送的报文，路由器把帧中继报文头的 BECN 标志位置为 1。若在一段时间内没有反方向的报文发送，路由器将自动发送 BECN 标志位为 1 的 Q.922A Test Reponse 报文给主叫 DTE。

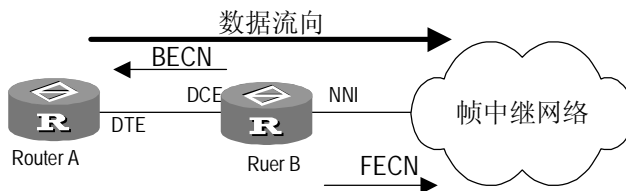


图5-9 帧中继拥塞管理示意图

5. 帧中继 DE 规则列表

在帧中继网络中，DE 标志位为 1 的报文会在拥塞发生时被优先丢弃。DE 规则列表应用于路由器的帧中继虚电路上，每个规则列表内包含多条 DE 规则。虚电路中发送的报文如果符合 DE 规则列表中的规则，则它的 DE 标志位将会被置 1，这类报文在网络发生拥塞时将会被优先丢弃。

5.2 帧中继 OoS 的配置

帧中继 QoS 的配置包括：

- | 创建并配置帧中继 class
- | 配置帧中继流量整形
- | 配置帧中继流量监管
- | 配置帧中继拥塞管理
- | 配置帧中继 DE 规则列表
- | 配置帧中继拥塞管理
- | 配置帧中继队列管理
- | 配置帧中继分片

5.2.1 创建和配置帧中继 class

VRP 系统把帧中继虚电路上的 QoS 服务整合在帧中继 class 上，提供了一个灵活、完整的帧中继流量控制和质量服务解决方案。在配置帧中继流量整形等 QoS 服务时，需要先创建一个帧中继 class，然后在这个帧中继 class 上配置各种 QoS 参数。这样一个帧中继 class 就相当于一套 QoS 网络服务方案。然后将帧中继 class 关联到一个帧中继虚电路上，就相当于将一套 QoS 服务方案应用到帧中继虚电路上。不同的虚电路可以使用不同的帧中继 class，也可以使用同一个帧中继 class。

帧中继 class 的配置包括：

- | 创建帧中继 class
- | 将帧中继 class 同帧中继接口或帧中继虚电路相关联
- | 配置帧中继 class 参数

1. 创建帧中继 class

请在系统视图下进行下列配置。

表5-1 创建/删除帧中继 class

操作	命令
创建帧中继 class	fr class <i>class-name</i>
删除帧中继 class	undo fr class <i>class-name</i>

缺省情况下，系统没有创建帧中继 class。

在使用本命令创建帧中继 class 之后，将进入帧中继 class 视图，用户可以在此视图下配置 CIR 等帧中继 class 参数。

2. 将帧中继 class 同帧中继接口或帧中继虚电路相关联

请在帧中继 DLCI 视图下进行下列配置。

表5-2 将帧中继 class 同帧中继接口或帧中继虚电路相关联

操作	命令
将帧中继 class 同帧中继接口或虚电路相关联	fr-class <i>class-name</i>
将帧中继 class 同帧中继接口或虚电路的关联取消	undo fr-class <i>class-name</i>

缺省情况下，没有帧中继 class 同帧中继虚电路相关联。

当帧中继虚电路提供 QoS 服务时，它将按照下面的顺序寻找对应的帧中继 class：

- (1) 使用和此帧中继虚电路相关联的帧中继 class。
- (2) 如果此帧中继虚电路属于帧中继子接口，使用帧中继子接口的帧中继 class。
- (3) 使用此帧中继虚电路所属的帧中继主接口的帧中继 class。

在使用命令 **fr-class** 时，假如指定的帧中继 class 不存在，此命令会先创建一个帧中继 class（但不会进入帧中继 class 视图），然后再将此帧中继 class 同当前接口或虚电路关联起来。

命令 **undo fr-class** 只会将指定的帧中继 class 和虚电路的关联取消，并不会删除实际的帧中继 class。此时如果用 **display current-configuration** 命令查看路由器的配置，仍然可以看见帧中继 class 的配置。如果要删除帧中继 class，请使用 **undo fr class** 命令。

3. 配置帧中继 class 参数

在帧中继 class 视图下，可以为帧中继流量整形、帧中继流量监管、帧中继拥塞管理、帧中继队列管理等 QoS 服务配置不同的参数。详细的参数设置请见下面各节里的内容。

5.2.2 配置帧中继流量整形

帧中继流量整形的配置包括：

- ┆ 使能帧中继流量整形
- ┆ 创建帧中继 class
- ┆ 将帧中继 class 同帧中继接口或帧中继虚电路相关联
- ┆ 配置帧中继流量整形帧中继 class 参数

1. 使能帧中继流量整形

请在同步串口视图下进行下列配置。

表5-3 使能/禁用帧中继流量整形功能

操作	命令
使能帧中继流量整形	fr traffic-shaping
禁用帧中继流量整形	undo fr traffic-shaping

缺省情况下，接口的帧中继流量整形功能没有被启用。

帧中继流量整形功能应用于路由器帧中继报文的发送接口上。通常情况下，它被应用于帧中继网络的 DTE 端。

& 说明：

帧中继流量整形不支持快转，需要关闭快转，帧中继流量整形才能生效。

2. 创建帧中继 class

具体配置步骤请参考“帧中继 OoS 的配置”中的“配置帧中继 class”。

3. 将帧中继 class 同帧中继接口或帧中继虚电路相关联

具体配置步骤请参考“帧中继 OoS 的配置”中的“配置帧中继 class”。

4. 配置帧中继流量整形的帧中继 class 参数

请在帧中继 class 视图下进行下列配置。

表5-4 配置帧中继流量整形帧中继 class 参数

操作	命令
设置帧中继虚电路的承诺突发流量	cbs [outbound] committed-burst-size
恢复帧中继虚电路承诺突发流量的缺省值	undo cbs [outbound]
设置帧中继虚电路的超出突发流量	ebs [outbound] excess-burst-size

操作	命令
恢复帧中继虚电路超出突发流量的缺省值	undo ebs [outbound]
设置帧中继虚电路的允许承诺信息速率	cir allow [outbound] <i>committed-information-rate</i>
恢复帧中继虚电路允许承诺信息速率的缺省值	undo cir allow [outbound]
设置帧中继虚电路的承诺信息速率	cir <i>committed-information-rate</i>
恢复帧中继虚电路承诺信息速率的缺省值	undo cir
使能帧中继流量整形的自适应流量调节功能	traffic-shaping adaptation { becn <i>percentage interface-congestion number</i> }
禁用帧中继流量整形的自适应流量调节功能	undo traffic-shaping adaptation { becn interface-congestion }

命令 **cbs**、**ebs**、**cir allow** 可以设置虚电路上输入和输出（**inbound** 和 **outbound**）两个方向的参数，但对帧中继流量整形只有 **outbound** 方向的参数有效。

& 说明：

在配置 CIR ALLOW 和 CBS 时，数值上 CBS 之值不应小于 CIR ALLOW 之值，否则可能会出现大报文无法发送的问题。

5.2.3 配置帧中继流量监管

帧中继流量监管的配置包括：

- ┆ 使能帧中继流量监管
- ┆ 创建帧中继 **class**
- ┆ 将帧中继 **class** 同帧中继接口或帧中继虚电路相关联
- ┆ 配置帧中继流量监管帧中继 **class** 参数

1. 使能帧中继流量监管

请在同步串口视图下进行下列配置。

表5-5 使能/禁用帧中继流量监管功能

操作	命令
使能帧中继流量监管	fr traffic-policing
禁用帧中继流量监管	undo fr traffic-policing

缺省情况下，接口的帧中继流量监管功能没有被启用。

帧中继流量监管功能应用于路由器帧中继报文的接收接口上。它只能被应用于帧中继网络的 DCE 端。

2. 创建帧中继 class

具体配置步骤请参考“帧中继 OoS 的配置”中的“配置帧中继 class”。

3. 将帧中继 class 同帧中继接口或帧中继虚电路相关联

具体配置步骤请参考“帧中继 OoS 的配置”中的“配置帧中继 class”。

4. 配置帧中继流量监管的帧中继 class 参数

请在帧中继 class 视图下进行下列配置。

表5-6 配置帧中继流量监管的帧中继 class 参数

操作	命令
设置帧中继虚电路的承诺突发流量	cbs [inbound] committed-burst-size
恢复帧中继虚电路承诺突发流量的缺省值	undo cbs [inbound]
设置帧中继虚电路的超出突发流量	ebs [inbound] excess-burst-size
恢复帧中继虚电路超出突发流量的缺省值	undo ebs [inbound]
设置帧中继虚电路的允许承诺信息速率	cir allow [inbound] committed-information-rate
恢复帧中继虚电路允许承诺信息速率的缺省值	undo cir allow [inbound]

命令 **cbs**、**ebs**、**cir allow** 可以设置虚电路上输入和输出（**inbound** 和 **outbound**）两个方向的参数，但对帧中继流量监管只有 **inbound** 方向的参数有效。

5.2.4 配置帧中继拥塞管理

对拥塞门限的设置，可以采用两种方式，即在指定的帧中继 class 里进行配置某条虚电路的拥塞门限，也可以在接口视图下对整个接口进行拥塞门限的配置。路由器根据帧中继接口或虚电路当前的队列长度占接口队列总长度的比例来判断接口是否发生拥塞。如果接口或虚电路当前队列长度与队列总长度之比大于用户设置的阈值，则路由器认为发生了拥塞，从而对报文进行丢弃等相应处理。

帧中继拥塞管理包括帧中继接口上的拥塞管理和帧中继虚电路上的拥塞管理两部分。

1. 配置帧中继接口的拥塞管理策略

请在同步串口视图下进行下列配置。

表5-7 配置帧中继接口的拥塞管理策略

操作	命令
使能帧中继接口在拥塞发生时丢弃 DE 标志位为 1 的报文	fr congestion-threshold de <i>queue-percentage</i>
禁止帧中继接口在拥塞发生时丢弃 DE 标志位为 1 的报文	undo fr congestion-threshold de
使能帧中继接口在拥塞发生时对 BECN 和 FECN 标志位进行处理	fr congestion-threshold ecn <i>queue-percentage</i>
禁止帧中继接口在拥塞发生时对 BECN 和 FECN 标志位进行处理	undo fr congestion-threshold ecn

缺省情况下，帧中继接口的拥塞管理功能没有启用。

当帧中继接口使能拥塞管理时，接口的队列类型只能为 FIFO 或 PVC PQ。

2. 配置帧中继虚电路的拥塞管理策略

请在帧中继 class 视图下进行下列配置。

表5-8 配置帧中继虚电路的拥塞管理策略

操作	命令
使能帧中继虚电路在拥塞发生时丢弃 DE 标志位为 1 的报文	congestion-threshold de<i>queue-percentage</i>
禁止帧中继虚电路在拥塞发生时丢弃 DE 标志位为 1 的报文	undo congestion-threshold de
使能帧中继虚电路在拥塞发生时对 BECN 和 FECN 标志位进行处理	congestion-threshold ecn <i>queue-percentage</i>
禁止帧中继虚电路在拥塞发生时对 BECN 和 FECN 标志位进行处理	undo congestion-threshold ecn

缺省情况下，帧中继虚电路的拥塞管理功能没有启用。

当帧中继虚电路使能拥塞管理时，虚电路的队列类型只能为 FIFO。

& 说明：

只有当虚电路所在接口使能了帧中继流量整形功能之后，虚电路的拥塞管理功能才能够起作用。

5.2.5 配置帧中继 DE 规则列表

1. 配置 DE 规则列表

请在系统视图下进行下列配置。

表5-9 配置 DE 规则列表

操作	命令
配置基于接口的 DE 规则列表	fr del <i>list-number inbound-interface type number</i>
删除基于接口的 DE 规则	undo fr del <i>list-number inbound-interface type number</i>
配置基于协议的 DE 规则列表	fr del <i>list-number protocol protocol [characteristic]</i>
删除基于协议的 DE 规则	undo fr del <i>list-number protocol protocol [characteristic]</i>

缺省情况下，没有定义 DE 规则列表。

一台路由器最多可以支持 10 个 DE 规则列表，在每个 DE 规则列表内最多可以拥有 100 条 DE 规则。

命令 **fr del inbound-interface** 和 **fr del protocol** 可以往一个 DE 规则列表中添加多个规则。命令 **undo fr del inbound-interface** 和 **undo fr del protocol** 每次只能删除一条 DE 规则，如果要删除一个 DE 规则列表，必须把列表中的所有 DE 规则全部删除。

2. 在帧中继虚电路上应用 DE 规则列表

请在同步串口视图下进行下列配置。

表5-10 在帧中继虚电路上应用 DE 规则列表

操作	命令
将 DE 规则列表应用到帧中继虚电路上	fr de del <i>list-number dlci dlci-number</i>
将 DE 规则列表从帧中继虚电路上删除	undo fr de del <i>list-number dlci dlci-number</i>

缺省情况下，帧中继虚电路上没有应用 DE 规则列表。

5.2.6 配置帧中继队列管理

1. 配置帧中继虚电路队列

当帧中继接口使能了帧中继流量整形之后，在此接口下的每条虚电路都将拥有一个独立的虚电路队列。如果帧中继接口没有使能帧中继流量整形，则虚电路将没有虚电路队列。

请在帧中继 **class** 视图下进行下列配置。

表5-11 配置帧中继虚电路的队列

操作	命令
设置帧中继虚电路的 FIFO 队列长度	fifo queue-length <i>queue-length</i>
恢复帧中继虚电路的 FIFO 队列长度的缺省值	undo fifo queue-length

操作	命令
设置帧中继虚电路的队列类型为 PQ	pq pql pql-index
恢复帧中继虚电路的队列类型为 FIFO	undo pq pql
设置帧中继虚电路的队列类型为 CQ	cq cql cql-index
恢复帧中继虚电路的队列类型为 FIFO	undo cq cql
设置帧中继虚电路的队列类型为 WFQ	wfq [congestive-discard-threshold [dynamic-queues]]
恢复帧中继虚电路的队列类型为 FIFO	undo wfq
设置帧中继虚电路的队列类型为 CBQ	apply policy outbound policy-name
取消应用 CBQ 为帧中继虚电路的队列	undo apply policy outbound
帧中继虚电路的队列类型为 RTPQ	rtpq start-port min-dest-port end-port max-dest-port bandwidth bandwidth
取消应用 RTPQ 为帧中继虚电路的队列	undo rtpq

缺省情况下，帧中继虚电路的队列类型为 FIFO。

当帧中继虚电路使能拥塞管理时，接口的队列类型只能为 FIFO。

队列 PQ、CQ、WFQ、CBQ 和 RTPQ 的配置请参考《VRP3.4 操作手册 QoS》部分。

2. 配置帧中继接口队列

在帧中继接口上可以配置的队列有：FIFO、PQ、CQ、WFQ、CBQ 和 RTPQ，这些都是通用 QoS 所拥有的队列。关于这些队列的配置请参考《VRP3.4 操作手册 QoS》部分。

帧中继接口还支持一种自己特有的队列 PVC PQ（PVC Interface Priority Queueing），此队列只能应用于帧中继接口。当帧中继接口使能帧中继流量整形后，接口的队列类型只能是 FIFO 或 PVC PQ；当帧中继接口使能拥塞管理后，接口队列类型只能为 FIFO 或 PVC PQ。

PVC PQ 队列根据不同的帧中继虚电路将报文分为四类

PVC PQ 队列拥有四个子队列，分别为高优先队列（**top**）、中优先队列（**middle**）、正常优先队列（**normal**）和低优先队列（**bottom**），它们的优先级依次降低。发送报文时将按照等级顺序依次发送，即先发送完所有 **top** 队列中的报文后，再发送所有 **middle** 队列中的报文，然后再发送所有 **normal** 队列中的报文，最后才发送 **bottom** 队列中的报文。接口上的每一个帧中继虚电路都拥有自己的 PVC PQ 队列等级，从这个虚电路发出的报文只能进入对应的 PVC PQ 队列。

请分别在接口视图或帧中继 **class** 视图下进行下列配置。

表5-12 配置 PVC PQ 队列

操作	命令
设置帧中继接口队列类型为 PVC PQ,同时设置 PVC PQ 各队列的长度（接口视图）	fr pvc-pq [<i>top-limit middle-limit normal-limit bottom-limit</i>]
恢复帧中继接口的队列类型为 FIFO（接口视图）	undo fr pvc-pq
设置帧中继虚电路的 PVC PQ 队列等级（帧中继 class 视图）	pvc-pq { <i>top</i> <i>middle</i> <i>normal</i> <i>bottom</i> }
恢复帧中继虚电路的 PVC PQ 队列等级为 normal （帧中继 class 视图）	undo pvc-pq

5.2.7 配置帧中继分片

VRP 系统支持 FRF.12 的 end-to-end 分片功能。

在低速帧中继线路上，大的数据报文将会造成传输时延的增大。帧中继分片特性可以将大的帧中继报文分割成几个小报文，从而可以保证在低速线路上数据也可以被低延迟的发送。

当语音与数据同传时，大数据报文的发送将长时间占用带宽，会造成语音报文被延时甚至丢弃，影响语音质量。配置帧中继分片的目的是尽量减少语音的延时，保证语音的实时性。配置分片后大的数据报文将被拆分为较小的数据分片，语音报文与拆分后的分片交替发送，保证语音报文及时均匀的得到处理，降低时延。

请在帧中继 class 视图下进行下列配置。

表5-13 配置帧中继分片

操作	命令
使能帧中继分片功能	fragment [<i>fragment-size</i>]
禁止帧中继分片功能	undo fragment [<i>fragment-size</i>]

缺省情况下，帧中继分片功能是禁止的。如果使能了帧中继功能而不指定分片大小，缺省的分片大小是 45 字节。

配置完成后，将需要应用分片功能的帧中继虚电路同此帧中继 class 关联，并使能帧中继流量整形，这时帧中继分片才会生效。

& 说明：

MFR 接口上不支持 FRF.12 的分片。如果两边都是 MFR 接口，且配置了 FRF.12 分片，则 FRF.12 分片不起作用，此时本端报文会完整发出，对端可以接收，在本端执行 ping 命令可以得到响应；如果本端是 MFR 接口，对端是普通帧中继接口（即封装了 FR 的 Serial 接口），则本端 FRF.12 分片不起作用，报文会完整发出，对端的 FRF.12 分片起作用。

5.3 帧中继 QoS 的显示和调试

在完成上述配置后，可在所有视图下执行 **display** 命令显示配置后帧中继的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **debugging** 命令可对帧中继进行调试。

表5-14 FR QoS 的显示和调试

操作	命令
查看帧中继 class 与接口（包括属于该接口的 dlcI、该接口下的子接口以及子接口下的 dlcI）的映射关系。	display fr class-map { fr-class <i>class-name</i> interface <i>interface-type</i> <i>interface-number</i> }
显示 DE 规则列表的内容	display fr del [<i>list-number</i>]
查看 FR QoS 的配置和统计信息	display fr pvc-info [interface <i>interface-type</i> <i>interface-number</i>] [<i>dlci-number</i>]
查看配置的帧中继路由的状态	display fr switch-table { all name <i>switch-name</i> }
查看接口应用 CBQ 的信息	display qos policy interface [<i>interface-type</i> <i>interface-number</i> [dlci <i>dlci-number</i> [outbound] inbound outbound]]
查看帧中继分片信息	display fr fragment-info [interface <i>interface-type</i> <i>interface-number</i>] [<i>dlci-number</i>]
查看帧中继收发数据统计信息	display fr statistics [interface <i>interface-type</i> <i>interface-number</i>]
使能 FR QoS 的拥塞管理调试功能	debugging fr congestion [interface <i>interface-type</i> <i>interface-number</i>]
禁止 FR QoS 的拥塞管理调试功能	undo debugging fr congestion [interface <i>interface-type</i> <i>interface-number</i>]
打开 FR QoS 的 DE 调试信息开关	debugging fr de [interface <i>interface-type</i> <i>interface-number</i>]
关闭 DE 调试信息开关	undo debugging fr de [interface <i>interface-type</i> <i>interface-number</i>]
打开 FR QoS 速率调整的调试信息开关	debugging fr transmit-rate [interface <i>interface-type</i> <i>interface-number</i>]
关闭速率调整的调试信息开关	undo debugging fr transmit-rate [interface <i>interface-type</i> <i>interface-number</i>]

5.4 帧中继 QoS 典型配置举例

5.4.1 帧中继流量整形配置举例

1. 配置需求

路由器 RouterA 通过接口 Serial4/0/0 连接至帧中继网络，要求路由器的平均发送速率为 96kbit/s，最大发送速率为 128kbit/s，最小发送速率为 32kbit/s，路由器具备流量自适应调整功能。要求使用 PQ 队列，保证所有来自 10.0.0.0 网段的 IP 报文可以优先通过。

2. 组网图

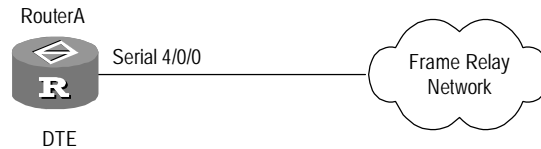


图5-10 帧中继流量整形组网图

3. 配置步骤

定义优先队列组 2001，要求所有来自 10.0.0.0 网段的 IP 报文可以最先通过。

```
[Quidway] acl number 2001
[Quidway-acl-basic-2001] rule permit source 10.0.0.0 0 0.255.255.255
[Quidway-acl-basic-2001] quit
[Quidway] qos pql 1 protocol ip acl 2001 queue top
```

创建帧中继 class 并配置帧中继流量整形参数。

```
[Quidway] fr class 96k
[Quidway-fr-class-96k] cir allow 96000
[Quidway-fr-class-96k] cir 32000
[Quidway-fr-class-96k] cbs 96000
[Quidway-fr-class-96k] ebs 32000
[Quidway-fr-class-96k] traffic-shaping adaptation becn 20
[Quidway-fr-class-96k] pq pql 1
[Quidway-fr-class-96k] quit
```

配置接口 Serial4/0/0，使能帧中继流量整形。

```
[Quidway] interface serial 4/0/0
[Quidway-Serial4/0/0] link-protocol fr
[Quidway-Serial4/0/0] ip address 1.1.1.1 255.255.255.0
[Quidway-Serial4/0/0] fr traffic-shaping
```

创建帧中继虚电路，将帧中继 class 同虚电路相关联。

```
[Quidway-Serial4/0/0] fr dlci 16
[Quidway-fr-dlci-Serial4/0/0-16] fr-class 96k
```

5.4.2 帧中继分片配置举例

1. 配置需求

路由器 RouterA 和 RouterB 通过帧中继网络相连, 使能帧中继分片功能 (FRF.12)。

2. 组网图

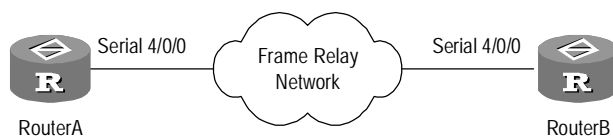


图5-11 FRF.12 典型组网图

3. 配置步骤

(1) 配置路由器 RouterA

配置帧中继 class test1

```
[Quidway] fr class test1
[Quidway-fr-class-test1] cir allow 64000
[Quidway-fr-class-test1] cbs 64000
[Quidway-fr-class-test1] cir 64000
[Quidway-fr-class-test1] fragment 80
[Quidway-fr-class-test1] quit
```

配置接口 Serial4/0/0

```
[Quidway] interface serial 4/0/0
[Quidway-Serial4/0/0] link-protocol fr
[Quidway-Serial4/0/0] ip address 10.1.1.2 255.0.0.0
```

创建 DLCI 16

```
[Quidway-Serial4/0/0] fr dlci 16
```

将名为 test1 的帧中继 class 应用到 DLCI 16 上

```
[Quidway-fr-dlci-Serial4/0/0-16] fr-class test1
```

(2) 配置路由器 RouterB

配置帧中继 class test1

```
[Quidway] fr class test1
[Quidway-fr-class-test1] cir allow 64000
[Quidway-fr-class-test1] cbs 64000
[Quidway-fr-class-test1] cir 64000
[Quidway-fr-class-test1] fragment 80
```

配置接口 Serial4/0/0

```
[Quidway] interface serial 4/0/0
[Quidway-Serial4/0/0] link-protocol fr
[Quidway-Serial4/0/0] ip address 10.1.1.1 255.0.0.0
```

创建 DLCI 16

```
[Quidway-Serial4/0/0] fr dlci 16
```

将名为 **test1** 的帧中继 class 应用到 DLCI 16 上

```
[Quidway-fr-dlci-Serial4/0/0-16] fr-class test1
```

```
[Quidway-fr-dlci-Serial4/0/0-16] quit
```

```
[Quidway-Serial4/0/0] quit
```


第6章 MPLS QoS

6.1 MPLS QoS 概述

MPLS 的 QoS 主要完成以下功能：

根据需要在 CE 上或 PE 上对业务流进行分类，例如：把业务流分为三类：语音、视频和数据。

PE 在给报文加 Label 时，把 IP 报文携带的 IP 优先级标记影射到标签的 CoS 域，这样原来由 IP 携带的类型信息，现在由标签携带。

在 PE 路由器之间，根据标签的 CoS 域，进行有差别的调度（如 PQ、WFQ、CBQ 等），即把携带标签的业务流在一条 LSP 上进行有差别的 QoS 的传送。

& 说明：

本章用户需要有 MPLS 相关知识背景。如需了解 MPLS 基本概念以及相关配置，请参考本书 MPLS 配置部分，本章仅涉及 MPLS QoS 的配置。

6.2 MPLS QoS 配置

配置 MPLS QoS 首先要进行 MPLS 的相关配置并指定为显示路由转发方式。MPLS 的详细配置请参见本书的 MPLS 配置部分。本章仅介绍 MPLS QoS 的配置。

MPLS QoS 的可以分为四种：

- | MPLS PQ
- | MPLS CQ
- | MPLS CBQ
- | MPLS CAR

下面对这四种 MPLS QoS 的配置分别进行说明。

6.2.1 配置 MPLS PQ

配置 MPLS PQ 有两个步骤。首先要根据 MPLS EXP 配置优先列表，然后在接口上应用此优先列表。相关说明可参考“拥塞管理”中的“PQ 配置”。

1. 根据 MPLS EXP 配置优先列表

根据 MPLS EXP 值配置优先列表，并使匹配的分组进入不同的优先队列。

请在系统视图进行下列配置。

表6-1 根据网络协议配置优先列表

操作	命令
根据网络协议配置优先列表	qos pql pql-index protocol mpls exp mpls-experimental-value queue { top middle normal bottom }
删除 pql-index 中相应的分类规则	undo qos pql pql-index protocol mpls exp mpls-experimental-value

优先队列的相关配置请参见3.1.1 2. PQ（优先队列，Priority Queuing）。

2. 在接口上应用优先列表组

将一组优先列表应用到接口上。对于同一个接口，本命令的重复使用将为接口设定新的优先列表组。

请在接口视图下进行下列配置。

表6-2 在接口上应用优先列表组

操作	命令
在接口上应用优先列表组	qos pq pql pql-index
将接口的拥塞管理策略恢复为 FIFO	undo qos pq

6.2.2 配置 MPLS CQ

配置 MPLS CQ 有两个步骤。首先要根据 MPLS EXP 配置定制列表，然后在接口上应用此定制列表。相关说明可参考“拥塞管理”中的“CQ 配置”。

1. 根据 MPLS EXP 配置定制列表

根据 MPLS EXP 配置定制列表，并使匹配的分组进入不同的定制队列。

请在系统视图下进行下列配置。

表6-3 根据网络协议配置定制列表

操作	命令
根据 MPLS EXP 配置定制列表	qos cql cql-index protocol mpls exp experimental-number queue queue-number
删除相应的分类规则	undo qos cql cql-index protocol mpls exp experimental-number

queue-number 取值为 0~16。关于定制队列的配置请参见3.1.1 3. CQ（定制队列，Custom Queuing）。

2. 在接口上应用定制列表

请在接口视图下进行下列配置。

表6-4 在接口上应用定制列表

操作	命令
在接口上应用定制列表	qos cq cql <i>cql-index</i>
将接口的拥塞管理策略恢复到 FIFO	undo qos cq

6.2.3 配置 MPLS CBQ

配置 MPLS CBQ 有四个步骤。第一，要定义类，根据 MPLS EXP 配置类的匹配规则；第二，要定义流行为，配置处理 MPLS EXP 域的方案；第三，定义一个 QoS 策略，为每个类指定具体的流行为；第四，在接口上应用此 QoS 策略。相关说明可参考“拥塞管理”中的“CBQ 配置”。

1. 配置匹配 mpls 报文的 exp 域的分类规则

MPLS QoS 允许用户在 PE 上通过 MPLS EXP 域来对 MPLS 报文进行分类并进入不同的队列，实现 QoS，IP 报文则不加改变地透明穿过 MPLS 网络。

首先要定义一个类并进入类视图，然后在类视图中配置匹配 mpls 报文的 exp 域的分类规则。

请在系统视图下进行下列配置。

表6-5 定义一个类并进入类视图

操作	命令
定义类并进入类映射视图	traffic classifier <i>tcl-name</i> [operator { and or }]
删除类并进入类映射视图	undo traffic classifier <i>tcl-name</i> [operator { and or }]

请在类视图下进行下列配置。

表6-6 匹配 mpls 的 exp 域的规则

操作	命令
定义匹配 mpls 的 exp 域的规则	if-match [not] mpls-exp { <i>mpls-experimental-value</i> }
删除匹配 mpls 的 exp 域的规则	undo if-match [not] mpls-exp

2. 设置 MPLS CBQ 流行为

首先在流行为视图下配置设置 MPLS EXP 域的值，然后在策略视图下将类与流行为关联，这样就可以对匹配类的报文进行 MPLS EXP 域的标记。

请在系统视图下进行下列配置。

表6-7 定义一个流行为并进入流行为视图

操作	命令
定义一个流行为并进入流行为视图	traffic behavior <i>behavior-name</i>
删除流行为	undo traffic behavior <i>behavior-name</i>

请在流行为视图下进行下列配置。

表6-8 设置 MPLS EXP 域的值来标记匹配的报文

操作	命令
设置 MPLS EXP 域的值来标记匹配的报文	remark mpls-exp <i>mpls-experimental-value</i>
取消 MPLS EXP 域的值	undo remark mpls-exp

3. 配置 MPLS CBQ 策略

首先要定义一个 QoS 策略名称，然后在 QoS 策略中为类指定流行为，即对不同类的报文标记不同的 EXP 值。

请在系统视图下进行下列配置。

表6-9 定义策略并进入策略视图

操作	命令
定义策略并进入策略视图	qos policy <i>policy-name</i>
删除指定策略	undo qos policy <i>policy-name</i>

请在策略视图下进行下列配置。

表6-10 在策略中为类指定流行为

操作	命令
在策略中为类指定采用的流行为	classifier <i>tcl-name</i> behavior <i>behavior-name</i>
取消指定类在策略中的使用	undo classifier <i>tcl-name</i>

tcl-name: 类名，必须是已经定义的类，可以是系统定义或用户定义类。

behavior-name: 必须是已定义的流行为名，可以是系统定义或用户定义流行为。

4. 应用 QoS 策略

请在接口视图或 ATM PVC 视图下进行下列配置。

表6-11 将接口或 ATM PVC 与所设置的策略相关联

操作	命令
在接口或 ATM PVC 应用关联的策略	qos apply policy <i>policy-name</i> { inbound outbound }
在接口或 ATM PVC 删除关联的策略	undo qos apply policy { inbound outbound }

6.2.4 配置 MPLS CAR

配置 MPLS CAR 有两个步骤。一是确定哪些报文需要实施监管，二是定义对这些报文的监管策略。确定哪些报文需要实施监管的方法可以使用访问控制列表（ACL），也可以使用 TP 列表（*carl-index*）。如果要对所有报文都进行监管，可以使用关键字 “**any**”。相关说明可参考“流量监管配置”。

1. 接口应用 TP 策略，对 MPLS 报文进行标记

在接口应用 TP 策略（CAR），对 MPLS 报文进行标记。

请在接口视图下进行下列配置。

表6-12 在接口应用 TP 策略，对 MPLS 报文进行标记

操作	命令
在接口应用 TP 策略，对 MPLS 报文进行标记	qos car inbound { any acl <i>acl-number</i> carl <i>carl-index</i> } cir <i>committed-information-rate</i> cbs <i>committed-burst-size</i> ebs <i>excess-burst-size</i> green action red action
取消在接口应用的 TP 策略	undo qos car inbound { any acl <i>acl-number</i> carl <i>carl-index</i> } cir <i>committed-information-rate</i> cbs <i>committed-burst-size</i> ebs <i>excess-burst-size</i>

action 的取值为：

- ▮ **remark-mpls-exp-continue** *new-mpls-exp*：设置新的 MPLS EXP 值 *new-mpls-exp*，并继续由下一个 CAR 策略处理，取值范围 0~7。
- ▮ **remark-mpls-exp-pass** *new-mpls-exp*：设置新的 MPLS EXP 值 *new-mpls-exp*，并发送数据包到目的地址，取值范围 0~7。

只能在 PE 的入接口上才可以设置 MPLS 报文的 EXP 域。如果入方向为 IP 报文，出方向封装为 MPLS 报文，则配置的 TP 策略（设置 MPLS 报文的 EXP 域）生效。设置 MPLS 报文的 EXP 域时，两层标签都要设置，但不修改 IP 头部中的 TOS 域。

6.3 MPLS QoS 典型配置举例

6.3.1 对同一 VPN 内的流进行 QoS 配置

1. 组网需求

在下面的组网图中，CE1 和 CE2 都属于 VPN1，PE1 与 P 之间的链路带宽为 2M，P 与 PE2 之间的链路带宽为 2M，要求对 VPN1 中优先级不同的流给予不同的 QoS 保证。

此举例的配置可分为两个主要部分：

首先在 CE1、PE1、P、PE2 和 CE2 进行 MPLS VPN 的配置：

- | PE1、P、PE2 之间运行 OSPF；
- | PE 与 CE 之间建立 MP-EBGP 邻居；
- | PE 与 PE 之间建立 MP-IBGP 邻居。

然后是在 PE1 和 P 上进行 MPLS QoS 的配置：

- | 在 PE1 的入接口 Ethernet1/1/0 上配置 QoS 策略，根据 MPLS 报文的 DSCP 属性，设置报文 EXP 域的值。
- | 在 P 路由器上，根据 MPLS 报文的 EXP 域值区分流，并配置基于流的队列 CBQ：对于 EXP 为 1 的流保证 10% 的带宽；对于 EXP 为 2 的流保证 20% 的带宽；对于 EXP 为 3 的流保证 30% 的带宽；而对于 EXP 为 4 的流，保证 40% 的带宽并保证时延。

& 说明：

MPLS VPN 的配置请参考本手册“MPLS 操作”部分，本节只描述 MPLS QoS 部分的配置。

2. 组网图

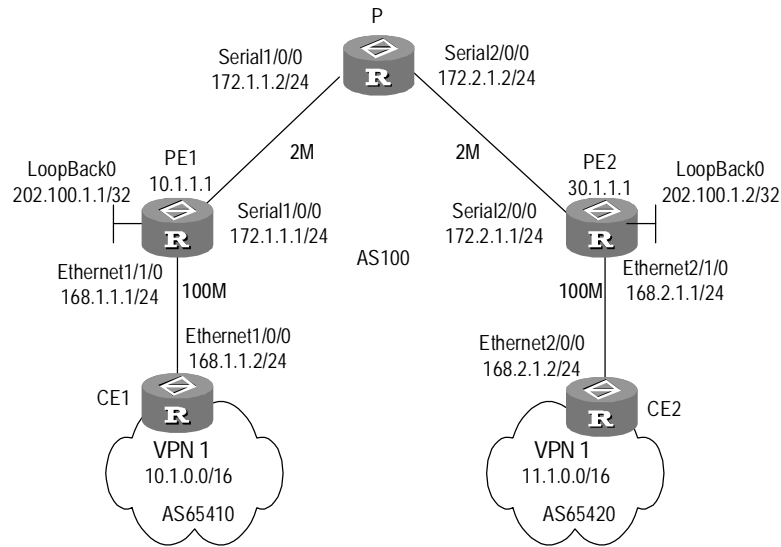


图6-1 MPLS QoS 组网图

3. 配置步骤

(1) PE1 的配置

定义四个类，分别匹配同一 VPN 内 DSCP 分别为 AF11、AF21、AF31 和 EF 的 MPLS 报文。

```
[PE1] traffic classifier af11
[PE1-classifier-af11] if-match dscp af11
[PE1-classifier-af11] traffic classifier af21
[PE1-classifier-af21] if-match dscp af21
[PE1-classifier-af21] traffic classifier af31
[PE1-classifier-af31] if-match dscp af31
[PE1-classifier-af31] traffic classifier efclass
[PE1-classifier-efclass] if-match dscp ef
[PE1-classifier-efclass] quit
```

定义四个流行为，设置 MPLS 报文 EXP 域的值。

```
[PE1] traffic behavior exp1
[PE1-behavior-exp1] remark mpls-exp 1
[PE1-behavior-exp1] traffic behavior exp2
[PE1-behavior-exp2] remark mpls-exp 2
[PE1-behavior-exp2] traffic behavior exp3
[PE1-behavior-exp3] remark mpls-exp 3
[PE1-behavior-exp3] traffic behavior exp4
[PE1-behavior-exp4] remark mpls-exp 4
[PE1-behavior-exp4] quit
```

定义 QoS 策略，为不同类的报文指定流行为，即对不同类的报文标记不同的 EXP 值。

```
[PE1] qos policy REMARK
[PE1-qospolicy-REMARK] classifier af11 behavior exp1
[PE1-qospolicy-REMARK] classifier af21 behavior exp2
[PE1-qospolicy-REMARK] classifier af31 behavior exp3
[PE1-qospolicy-REMARK] classifier efclass behavior exp4
[PE1-qospolicy-REMARK] quit
```

在 MPLS 网络的 PE 路由器入接口上应用已定义的 QoS 策略。

```
[PE1] interface ethernet 1/1/0
[PE1-Ethernet1/1/0] qos apply policy REMARK inbound
[PE1-Ethernet1/1/0] quit
```

(2) P 的配置

定义四个类，分别匹配 EXP 域为 1、2、3 和 4 的 MPLS 报文。

```
[P] traffic classifier EXP1
[P-classifier-EXP1] if-match mpls-exp 1
[P-classifier-EXP1] traffic classifier EXP2
[P-classifier-EXP2] if-match mpls-exp 2
[P-classifier-EXP2] traffic classifier EXP3
[P-classifier-EXP3] if-match mpls-exp 3
[P-classifier-EXP3] traffic classifier EXP4
[P-classifier-EXP4] if-match mpls-exp 4
[P-classifier-EXP4] quit
```

定义流行为，为不同的流设置不同的带宽和时延保证。

```
[P] traffic behavior AF11
[P-behavior-AF11] queue af bandwidth pct 10
[P-behavior-AF11] traffic behavior AF21
[P-behavior-AF21] queue af bandwidth pct 20
[P-behavior-AF21] traffic behavior AF31
[P-behavior-AF31] queue af bandwidth pct 30
[P-behavior-AF31] traffic behavior EF
[P-behavior-EF] queue ef bandwidth pct 40
[P-behavior-EF] quit
```

定义 QoS 策略，使符合流分类策略的 4 条数据流满足：EXP1 流保证 10%带宽；EXP2 流保证 20%带宽；EXP3 流保证 30%带宽；EXP4 流保证 40%带宽并保证时延。

```
[P] qos policy QUEUE
[P-qospolicy-QUEUE] classifier EXP1 behavior AF11
[P-qospolicy-QUEUE] classifier EXP2 behavior AF21
```



```
[P-qospolicy-QUEUE] classifier EXP3 behavior AF31
[P-qospolicy-QUEUE] classifier EXP4 behavior EF
[P-qospolicy-QUEUE] quit
```

将 QoS 策略应用在 P 路由器 Serial2/0/0 接口的出方向上。

```
[P] interface serial 2/0/0
[P-Serial2/0/0] qos apply policy QUEUE outbound
```

配置完成后，VPN1 中的流量在发生拥塞时，DSCP 域为 af11、af21、af31、ef 的流量接收比例为 1:2:3:4，其中，ef 流比其他 3 条流的延时都小。