H3C MSR 系列路由器

ACL 和 QoS 配置指导(V7)

杭州华三通信技术有限公司
http://www.h3c.com.cn

资料版本：6W103-20140512
产品版本：MSR-CMW710-R0105

前 言

H3C MSR 系列路由器 配置指导(V7)共分为十五本手册，介绍了 MSR 系列路由器各软件特性的原理及其配置方法，包含原理简介、配置任务描述和配置举例。《ACL 和 QoS 配置指导》主要介绍 QoS 相关协议的原理和配置，包括流分类、流量监管、流量整形、QoS 策略、拥塞管理、拥塞避免、MPLS QoS 等。

前言部分包含如下内容：

适用款型

本手册所描述的内容适用于 MSR 系列路由器中的如下款型：

款型	
MSR 2600	MSR 26-30
MSR 3600	MSR 36-10
	MSR 36-20
	MSR 36-40
	MSR 36-60
	MSR3600-28
	MSR3600-51
MSR 5600	MSR 56-60
	MSR 56-80

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[]	表示用“[]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... }*	表示从多个选项中至少选取一个。
[x | y | ...]*	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
说明	对操作内容的描述进行必要的补充和说明。
窍门	配置、操作、或使用设备的技巧、小窍门。

3. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。

4. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

产品配套资料

H3C MSR 系列路由器的配套资料包括如下部分：

大类	资料名称	内容介绍
产品知识介绍	路由器产品彩页	帮助您了解产品的主要规格参数及亮点
硬件描述与安装	路由器安装指导	帮助您详细了解设备硬件规格和安装方法，指导您对设备进行安装
	MSR 系列路由器接口模块手册	帮助您详细了解单板的硬件规格
业务配置	MSR 系列路由器配置指导(V7)	帮助您掌握设备软件功能的配置方法及配置步骤
	MSR 系列路由器命令参考(V7)	详细介绍设备的命令，相当于命令字典，方便您查阅各个命令的功能
运行维护	路由器版本说明书	帮助您了解产品版本的相关信息（包括：版本配套说明、兼容性说明、特性变更说明、技术支持信息）及软件升级方法

资料获取方式

您可以通过H3C网站（www.h3c.com.cn）获取最新的产品资料：

H3C 网站与产品资料相关的主要栏目介绍如下：

- [服务支持/文档中心]：可以获取硬件安装类、软件升级类、配置类或维护类等产品资料。
- [产品技术]：可以获取产品介绍和技术介绍的文档，包括产品相关介绍、技术介绍、技术白皮书等。
- [解决方案]：可以获取解决方案类资料。
- [服务支持/软件下载]：可以获取与软件版本配套的资料。

技术支持

用户支持邮箱：service@h3c.com

技术支持热线电话：400-810-0504（手机、固话均可拨打）

网址：http://www.h3c.com.cn

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 ACL

1.1 ACL简介

ACL（Access Control List，访问控制列表）是一或多条规则的集合，用于识别报文流。这里的规则是指描述报文匹配条件的判断语句，匹配条件可以是报文的源地址、目的地址、端口号等。网络设备依照这些规则识别出特定的报文，并根据预先设定的策略对其进行处理。

ACL可以应用在诸多领域，其中最基本的就是应用ACL进行报文过滤，具体配置过程请参见“1.3.5 应用ACL进行报文过滤”。此外，ACL还可应用于诸如路由、安全、QoS等业务中，有关ACL在这些业务中的具体应用方式，请参见相关的配置指导。

提示

ACL 本身只能识别报文，而无法对识别出的报文进行处理，对这些报文的具体处理方式由应用 ACL 的业务模块来决定。

1.1.1 ACL的编号和名称

用户在创建ACL时必须为其指定编号，不同的编号对应不同类型的ACL，如 表 1-1 所示；同时，为了便于记忆和识别，用户在创建ACL时还可选择是否为其设置名称。ACL一旦创建，便不允许用户再为其设置名称、修改或删除其原有名称。

当 ACL 创建完成后，用户就可以通过指定编号或名称的方式来指定该 ACL，以便对其进行操作。

说明

基本 ACL、高级 ACL 的编号和名称各在其适用的 IP 版本（IPv4 和 IPv6）中唯一。

1.1.2 ACL的分类

根据规则制订依据的不同，可以将ACL分为如 表 1-1 所示的几种类型。

表1-1 ACL 的分类

ACL 类型	编号范围	适用的 IP 版本	规则制订依据
基本ACL	2000～2999	IPv4	报文的源IPv4地址
		IPv6	报文的源IPv6地址
高级ACL	3000～3999	IPv4	报文的源IPv4地址、目的IPv4地址、报文优先级、IPv4承载的协议类型及特性等三、四层信息
		IPv6	报文的源IPv6地址、目的IPv6地址、报文优先级、IPv6承载的协议类型及特性等三、四层信息

ACL 类型	编号范围	适用的 IP 版本	规则制订依据
二层ACL	4000～4999	-	报文的源MAC地址、目的MAC地址、802.1p优先级、链路层协议类型等二层信息

1.1.3 ACL的规则匹配顺序

当一个 ACL 中包含多条规则时，报文会按照一定的顺序与这些规则进行匹配，一旦匹配上某条规则便结束匹配过程。ACL 的规则匹配顺序有以下两种：

- 配置顺序：按照规则编号由小到大进行匹配。
- 自动排序：按照“深度优先”原则由深到浅进行匹配，各类型ACL的“深度优先”排序法则如表 1-2 所示。

表1-2 各类型 ACL 的“深度优先”排序法则

ACL 类型	“深度优先”排序法则
IPv4基本ACL	(1) 先判断规则的匹配条件中是否包含 VPN 实例，包含者优先 (2) 如果 VPN 实例的包含情况相同，再比较源 IPv4 地址范围，较小者优先 (3) 如果源 IPv4 地址范围也相同，再比较配置的先后次序，先配置者优先
IPv4高级ACL	(1) 先判断规则的匹配条件中是否包含 VPN 实例，包含者优先 (2) 如果 VPN 实例的包含情况相同，再比较协议范围，指定有 IPv4 承载的协议类型者优先 (3) 如果协议范围也相同，再比较源 IPv4 地址范围，较小者优先 (4) 如果源 IPv4 地址范围也相同，再比较目的 IPv4 地址范围，较小者优先 (5) 如果目的 IPv4 地址范围也相同，再比较四层端口（即 TCP/UDP 端口）号的覆盖范围，较小者优先 (6) 如果四层端口号的覆盖范围无法比较，再比较配置的先后次序，先配置者优先
IPv6基本ACL	(1) 先判断规则的匹配条件中是否包含 VPN 实例，包含者优先 (2) 如果 VPN 实例的包含情况相同，再比较源 IPv6 地址范围，较小者优先 (3) 如果源 IPv6 地址范围也相同，再比较配置的先后次序，先配置者优先
IPv6高级ACL	(1) 先判断规则的匹配条件中是否包含 VPN 实例，包含者优先 (2) 如果 VPN 实例的包含情况相同，再比较协议范围，指定有 IPv6 承载的协议类型者优先 (3) 如果协议范围相同，再比较源 IPv6 地址范围，较小者优先 (4) 如果源 IPv6 地址范围也相同，再比较目的 IPv6 地址范围，较小者优先 (5) 如果目的 IPv6 地址范围也相同，再比较四层端口（即 TCP/UDP 端口）号的覆盖范围，较小者优先 (6) 如果四层端口号的覆盖范围无法比较，再比较配置的先后次序，先配置者优先
二层ACL	(1) 先比较源 MAC 地址范围，较小者优先 (2) 如果源 MAC 地址范围相同，再比较目的 MAC 地址范围，较小者优先 (3) 如果目的 MAC 地址范围也相同，再比较配置的先后次序，先配置者优先

说明

- 比较 IPv4 地址范围的大小，就是比较 IPv4 地址通配符掩码中“0”位的多少：“0”位越多，范围越小。通配符掩码（又称反向掩码）以点分十进制表示，并以二进制的“0”表示“匹配”，“1”表示“不关心”，这与子网掩码恰好相反，譬如子网掩码 255.255.255.0 对应的通配符掩码就是

0.0.0.255。此外，通配符掩码中的“0”或“1”可以是不连续的，这样可以更加灵活地进行匹配，譬如 0.255.0.255 就是一个合法的通配符掩码。

- 比较 IPv6 地址范围的大小，就是比较 IPv6 地址前缀的长短：前缀越长，范围越小。
- 比较 MAC 地址范围的大小，就是比较 MAC 地址掩码中“1”位的多少：“1”位越多，范围越小。

1.1.4 ACL的步长

ACL 中的每条规则都有自己的编号，这个编号在该 ACL 中是唯一的。在创建规则时，可以手工为其指定一个编号，如未手工指定编号，则由系统为其自动分配一个编号。由于规则的编号可能影响规则匹配的顺序，因此当由系统自动分配编号时，为了方便后续在已有规则之前插入新的规则，系统通常会在相邻编号之间留下一定的空间，这个空间的大小（即相邻编号之间的差值）就称为 ACL 的步长。譬如，当步长为 5 时，系统会将编号 0、5、10、15……依次分配给新创建的规则。

系统为规则自动分配编号的方式如下：系统从 0 开始，按照步长自动分配一个大于现有最大编号的最小编号。譬如原有编号为 0、5、9、10 和 12 的五条规则，步长为 5，此时如果创建一条规则且不指定编号，那么系统将自动为其分配编号 15。

如果步长发生了改变，ACL 内原有全部规则的编号都将自动从 0 开始按新步长重新排列。譬如，某 ACL 内原有编号为 0、5、9、10 和 15 的五条规则，当修改步长为 2 之后，这些规则的编号将依次变为 0、2、4、6 和 8。

1.1.5 ACL对分片报文的处理

传统的报文过滤并不处理所有的分片报文，只对分片报文的首个分片进行匹配处理，而对后续分片一律放行。这样，网络攻击者可以构造后续的分片报文进行流量攻击，从而带来了安全隐患。为提高网络安全性，ACL 规则缺省会匹配所有报文（包括非分片报文和分片报文的每个分片）。同时，为了提高匹配效率，用户也可以对此匹配策略进行修改，譬如可指定规则仅对分片报文的非首个分片有效等。

1.2 ACL配置任务简介

表1-3 ACL 配置任务简介

配置任务	说明	详细配置
配置基本ACL	三者至少选其一	1.3.1
配置高级ACL		1.3.2
配置二层ACL		1.3.3
复制ACL	可选	1.3.4
应用ACL进行报文过滤	可选	1.3.5

1.3 配置ACL

1.3.1 配置基本ACL

1. 配置IPv4 基本ACL

IPv4 基本 ACL 根据报文的源 IP 地址来制订规则，对 IPv4 报文进行匹配。

表1-4 配置 IPv4 基本 ACL

操作	命令	说明
进入系统视图	**system-view**	-
创建IPv4基本ACL，并进入IPv4基本ACL视图	**acl number** *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]	缺省情况下，不存在任何ACL IPv4基本ACL的编号范围为2000～2999 如果在创建IPv4基本ACL时为其设置了名称，则也可使用**acl name** *acl-name*命令进入其视图
（可选）配置ACL的描述信息	**description** *text*	缺省情况下，ACL没有任何描述信息
（可选）配置规则编号的步长	**step** *step-value*	缺省情况下，规则编号的步长为5
创建规则	**rule** [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *	缺省情况下，IPv4基本ACL内不存在任何规则 **logging**参数需要使用该ACL的模块支持日志记录功能，例如报文过滤
（可选）为指定规则配置描述信息	**rule** *rule-id* **comment** *text*	缺省情况下，规则没有任何描述信息

2. 配置IPv6 基本ACL

IPv6 基本 ACL 根据报文的源 IPv6 地址来制订规则，对 IPv6 报文进行匹配。

表1-5 配置 IPv6 基本 ACL

操作	命令	说明
进入系统视图	**system-view**	-
创建IPv6基本ACL，并进入IPv6基本ACL视图	**acl ipv6 number** *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]	缺省情况下，不存在任何ACL IPv6基本ACL的编号范围为2000～2999 如果在创建IPv6基本ACL时为其设置了名称，则也可使用**acl ipv6 name** *acl-name*命令进入其视图
（可选）配置ACL的描述信息	**description** *text*	缺省情况下，ACL没有任何描述信息
（可选）配置规则编号的步长	**step** *step-value*	缺省情况下，规则编号的步长为5

操作	命令	说明
创建规则	**rule** [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **routing** [**type** *routing-type*] | **source** { *source-address source-prefix* | *source-address/source-prefix* | **any** } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *	缺省情况下，IPv6基本ACL内不存在任何规则 **logging**参数需要使用该ACL的模块支持日志记录功能，例如报文过滤
（可选）为指定规则配置描述信息	**rule** *rule-id* **comment** *text*	缺省情况下，规则没有任何描述信息

1.3.2 配置高级ACL

1. 配置IPv4 高级ACL

IPv4 高级 ACL 可根据报文的源 IP 地址、目的 IP 地址、报文优先级、IP 承载的协议类型及特性（如 TCP/UDP 的源端口和目的端口、TCP 报文标识、ICMP 协议的消息类型和消息码等）等信息来制定规则，对 IPv4 报文进行匹配。用户可利用 IPv4 高级 ACL 制订比 IPv4 基本 ACL 更准确、丰富、灵活的规则。

表1-6 配置 IPv4 高级 ACL

操作	命令	说明
进入系统视图	**system-view**	-
创建IPv4高级ACL，并进入IPv4高级ACL视图	**acl number** *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]	缺省情况下，不存在任何ACL IPv4高级ACL的编号范围为3000～3999 如果在创建IPv4高级ACL时为其设置了名称，则也可使用**acl name** *acl-name*命令进入其视图
（可选）配置ACL的描述信息	**description** *text*	缺省情况下，ACL没有任何描述信息
（可选）配置规则编号的步长	**step** *step-value*	缺省情况下，规则编号的步长为5
创建规则	**rule** [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-address dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **logging** | **source** { *source-address source-wildcard* | **any** } | **source-port** *operator port1* [*port2*] } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *	缺省情况下，IPv4高级ACL内不存在任何规则 **logging**参数需要使用该ACL的模块支持日志记录功能，例如报文过滤
（可选）为指定规则配置描述信息	**rule** *rule-id* **comment** *text*	缺省情况下，规则没有任何描述信息

2. 配置IPv6 高级ACL

IPv6 高级 ACL 可根据报文的源 IPv6 地址、目的 IPv6 地址、报文优先级、IPv6 承载的协议类型及特性（如 TCP/UDP 的源端口和目的端口、TCP 报文标识、ICMPv6 协议的消息类型和消息码等）等信息来制定规则，对 IPv6 报文进行匹配。用户可利用 IPv6 高级 ACL 制订比 IPv6 基本 ACL 更准确、丰富、灵活的规则。

表1-7 配置 IPv6 高级 ACL

操作	命令	说明
进入系统视图	**system-view**	-
创建IPv6高级ACL，并进入IPv6高级ACL视图	**acl ipv6 number** *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]	缺省情况下，不存在任何ACL IPv6高级ACL的编号范围3000～3999 如果在创建IPv6高级ACL时为其设置了名称，则也可使用**acl ipv6 name** *acl-name*命令进入其视图
（可选）配置ACL的描述信息	**description** *text*	缺省情况下，ACL没有任何描述信息
（可选）配置规则编号的步长	**step** *step-value*	缺省情况下，规则编号的步长为5
创建规则	**rule** [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** } | **destination-port** *operator port1* [*port2*] | **dscp** *dscp* | **flow-label** *flow-label-value* | **fragment** | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **logging** | **routing** [**type** *routing-type*] | **hop-by-hop** [**type** *hop-type*] | **source** { *source-address source-prefix* | *source-address/source-prefix* | **any** } | **source-port** { *operator port1* [*port2*] } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *	缺省情况下，IPv6高级ACL内不存在任何规则 **logging**参数需要使用该ACL的模块支持日志记录功能，例如报文过滤
（可选）为指定规则配置描述信息	**rule** *rule-id* **comment** *text*	缺省情况下，规则没有任何描述信息

1.3.3 配置二层ACL

二层 ACL 可根据报文的源 MAC 地址、目的 MAC 地址、802.1p 优先级、链路层协议类型等二层信息来制订规则，对报文进行匹配。

表1-8 配置二层 ACL

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
创建二层ACL，并进入二层ACL视图	**acl number** *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]	缺省情况下，不存在任何ACL 二层ACL的编号范围为4000～4999 如果在创建二层ACL时为其设置了名称，则也可使用**acl name** *acl-name*命令进入其视图
（可选）配置ACL的描述信息	**description** *text*	缺省情况下，ACL没有任何描述信息
（可选）配置规则编号的步长	**step** *step-value*	缺省情况下，规则编号的步长为5
创建规则	**rule** [*rule-id*] { **deny** | **permit** } [**cos** *vlan-pri* | **counting** | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *	缺省情况下，二层ACL内不存在任何规则
（可选）为指定规则配置描述信息	**rule** *rule-id* **comment** *text*	缺省情况下，规则没有任何描述信息

1.3.4 复制ACL

用户可通过复制一个已存在的 ACL（即源 ACL），来生成一个新的同类型 ACL（即目的 ACL）。除了 ACL 的编号和名称不同外，目的 ACL 与源 ACL 完全相同。

提示

目的 ACL 要与源 ACL 的类型相同，且目的 ACL 必须不存在，否则将导致复制失败。

表1-9 复制 ACL

操作	命令	说明
进入系统视图	**system-view**	-
复制并生成一个新的ACL	**acl** [**ipv6**] **copy** { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }	-

1.3.5 应用ACL进行报文过滤

ACL 最基本的应用就是进行报文过滤，即通过将 ACL 规则应用到指定接口的入或出方向上，从而对该接口收到或发出的报文进行过滤。

1. 在接口上应用ACL进行报文过滤

表1-10 在接口上应用 ACL 进行报文过滤

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
在接口上应用ACL进行报文过滤	**packet-filter** [**ipv6**] { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }	缺省情况下，接口不对报文进行过滤

说明

一个接口在一个方向上最多可应用 32 个 ACL 进行报文过滤。

2. 在域间实例上应用ACL进行报文过滤

表1-11 在域间实例上应用 ACL 进行报文过滤

操作	命令	说明
进入系统视图	**system-view**	-
进入域间实例视图	**interzone source** *source-zone-name* **destination** *destination-zone-name*	-
在域间实例上应用ACL进行报文过滤	**packet-filter** [**ipv6**] { *acl-number* | **name** *acl-name* }	缺省情况下，域间实例不对报文进行过滤

说明

一个域间实例上最多可应用 32 个 ACL 进行报文过滤。

3. 配置报文过滤日志的生成与发送周期

在配置了报文过滤日志的生成与发送周期之后，设备将周期性地生成报文过滤日志信息并发送到信息中心，包括该周期内被匹配的报文数量以及所使用的 ACL 规则。关于信息中心的详细介绍请参见“网络管理和监控配置指导”中的“信息中心”。

表1-12 配置报文过滤日志的生成与发送周期

操作	命令	说明
进入系统视图	**system-view**	-
配置报文过滤日志的生成与发送周期	**acl** [**ipv6**] **logging interval** *interval*	缺省情况下，报文过滤日志的生成与发送周期为0分钟，即不记录报文过滤的日志

4. 配置报文过滤的缺省动作

系统缺省的报文过滤动作为 Permit，即允许未匹配上 ACL 规则的报文通过。通过本配置可更改报文过滤的缺省动作为 Deny，即禁止未匹配上 ACL 规则的报文通过。

表1-13 配置报文过滤的缺省动作为 deny

操作	命令	说明
进入系统视图	**system-view**	-
配置报文过滤的缺省动作为Deny	**packet-filter default deny**	缺省情况下，报文过滤的缺省动作为Permit，即允许未匹配上ACL规则的报文通过

1.4 ACL显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示 ACL 配置后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 ACL 的统计信息。

表1-14 ACL 显示和维护

配置	命令
显示ACL的配置和运行情况	**display acl** [**ipv6**] { *acl-number* | **all** | **name** *acl-name* }
显示ACL在报文过滤中的应用情况（MSR 2600/MSR 3600）	**display packet-filter** { **interface** [*interface-type interface-number*] [**inbound** | **outbound**] | **interzone** [**source** *source-zone-name* **destination** *destination-zone-name*] }
显示ACL在报文过滤中的应用情况（MSR 5600）	**display packet-filter** { **interface** [*interface-type interface-number*] [**inbound** | **outbound**] | **interzone** [**source** *source-zone-name* **destination** *destination-zone-name*] [**slot** *slot-number*] }
显示ACL在报文过滤中应用的统计信息以及报文过滤缺省动作的统计信息	**display packet-filter statistics** { **interface** *interface-type interface-number* { **inbound** | **outbound** } [**default** | [**ipv6**] { *acl-number* | **name** *acl-name* }] | **interzone source** *source-zone-name* **destination** *destination-zone-name* [[**ipv6**] { *acl-number* | **name** *acl-name* }] } [**brief**]
显示ACL在报文过滤中应用的累加统计信息	**display packet-filter statistics sum** { **inbound** | **outbound** } [**ipv6**] { *acl-number* | **name** *acl-name* } [**brief**]
显示ACL在报文过滤中的详细应用情况（MSR 2600/MSR 3600）	**display packet-filter verbose** { **interface** *interface-type interface-number* { **inbound** | **outbound** } | **interzone source** *source-zone-name* **destination** *destination-zone-name* } [[**ipv6**] { *acl-number* | **name** *acl-name* }]
显示ACL在报文过滤中的详细应用情况（MSR 5600）	**display packet-filter verbose** { **interface** *interface-type interface-number* { **inbound** | **outbound** } | **interzone source** *source-zone-name* **destination** *destination-zone-name* } [[**ipv6**] { *acl-number* | **name** *acl-name* }] [**slot** *slot-number*]
清除ACL的统计信息	**reset acl** [**ipv6**] **counter** { *acl-number* | **all** | **name** *acl-name* }
清除ACL在报文过滤中应用的统计信息（包括累加统计信息）以及报文过滤缺省动作的统计信息	**reset packet-filter statistics** { **interface** [*interface-type interface-number*] { **inbound** | **outbound** } [**default** | [**ipv6**] { *acl-number* | **name** *acl-name* }] | **interzone** [**source** *source-zone-name* **destination** *destination-zone-name*] [**ipv6**] { *acl-number* | **name** *acl-name* }] }

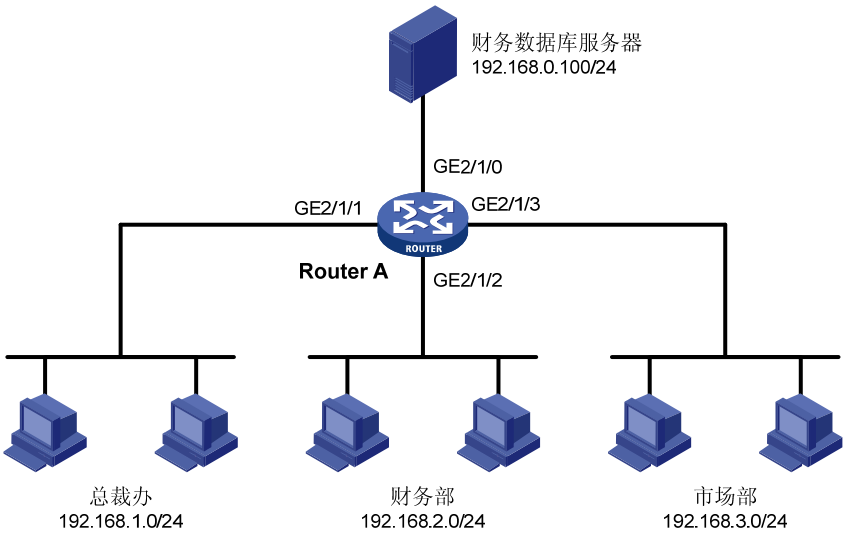
1.5 ACL典型配置举例

1. 组网需求

- 某公司内的各部门之间通过 Router A 实现互连，该公司的工作时间为每周工作日的 8 点到 18 点。
- 通过配置，允许总裁办在任意时间、财务部在工作时间访问财务数据库服务器，禁止其它部门在任何时间、财务部在非工作时间访问该服务器。

2. 组网图

图1-1 ACL 典型配置组网图



3. 配置步骤

创建名为 work 的时间段，其时间范围为每周工作日的 8 点到 18 点。

```
<RouterA> system-view
[RouterA] time-range work 08:0 to 18:00 working-day
```

创建 IPv4 高级 ACL 3000，并制订如下规则：允许总裁办在任意时间、财务部在工作时间访问财务数据库服务器，禁止其它部门在任何时间、财务部在非工作时间访问该服务器。

```
[RouterA] acl number 3000
[RouterA-acl-adv-3000] rule permit ip source 192.168.1.0 0.0.0.255 destination 192.168.0.100
0
[RouterA-acl-adv-3000] rule permit ip source 192.168.2.0 0.0.0.255 destination 192.168.0.100
0 time-range work
[RouterA-acl-adv-3000] rule deny ip source any destination 192.168.0.100 0
[RouterA-acl-adv-3000] quit
```

应用 IPv4 高级 ACL 3000 对接口 GigabitEthernet2/1/0 出方向上的报文进行过滤。

```
[RouterA] interface gigabitethernet 2/1/0
[RouterA-GigabitEthernet2/1/0] packet-filter 3000 outbound
[RouterA-GigabitEthernet2/1/0] quit
```

4. 验证配置

配置完成后，在各部门的 PC（假设均为 Windows XP 操作系统）上可以使用 **ping** 命令检验配置效果，在 Router A 上可以使用 **display acl** 命令查看 ACL 的配置和运行情况。例如在工作时间：

在财务部的 PC 上检查到财务数据库服务器是否可达。

```
C:\> ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Reply from 192.168.0.100: bytes=32 time=1ms TTL=255
Reply from 192.168.0.100: bytes=32 time<1ms TTL=255
Reply from 192.168.0.100: bytes=32 time<1ms TTL=255
Reply from 192.168.0.100: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

由此可见，财务部的 PC 能够在工作时间访问财务数据库服务器。

在市场部的 PC 上检查财务数据库服务器是否可达。

```
C:\> ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

由此可见，市场部的 PC 不能在工作时间访问财务数据库服务器。

查看 IPv4 高级 ACL 3000 的配置和运行情况。

```
[RouterA] display acl 3000
Advanced ACL  3000, named -none-, 3 rules,
ACL's step is 5
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.0.100 0
 rule 5 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.0.100 0 time-range work
(4 times matched) (Active)
 rule 10 deny ip destination 192.168.0.100 0 (4 times matched)
```

由此可见，由于目前是工作时间，因此规则 5 是生效的；且由于之前使用了 **ping** 命令的缘故，规则 5 和规则 10 分别被匹配了 4 次。

目 录

1 QoS简介

1.1 概述

QoS 即服务质量。对于网络业务，影响服务质量的因素包括传输的带宽、传送的时延、数据的丢包率等。在网络中可以通过保证传输的带宽、降低传送的时延、降低数据的丢包率以及时延抖动等措施来提高服务质量。

网络资源总是有限的，只要存在抢夺网络资源的情况，就会出现服务质量的要求。服务质量是相对网络业务而言的，在保证某类业务的服务质量的同时，可能就是在损害其它业务的服务质量。例如，在网络总带宽固定的情况下，如果某类业务占用的带宽越多，那么其他业务能使用的带宽就越少，可能会影响其他业务的使用。因此，网络管理者需要根据各种业务的特点来对网络资源进行合理的规划和分配，从而使网络资源得到高效利用。

下面从 QoS 服务模型出发，对目前使用最多、最成熟的一些 QoS 技术逐一进行描述。在特定的环境下合理地使用这些技术，可以有效地提高服务质量。

1.2 QoS服务模型简介

通常 QoS 提供以下三种服务模型：

- Best-Effort service（尽力而为服务模型）
- Integrated service（综合服务模型，简称 IntServ）
- Differentiated service（区分服务模型，简称 DiffServ）

1.2.1 Best-Effort 服务模型

Best-Effort 是一个单一的服务模型，也是最简单的服务模型。对 Best-Effort 服务模型，网络尽最大的可能性来发送报文。但对时延、可靠性等性能不提供任何保证。

Best-Effort 服务模型是网络的缺省服务模型，通过 FIFO 队列来实现。它适用于绝大多数网络应用，如 FTP、E-Mail 等。

1.2.2 IntServ 服务模型

IntServ 是一个综合服务模型，它可以满足多种 QoS 需求。该模型使用 RSVP 协议，RSVP 运行在从源端到目的端的每个设备上，可以监视每个流，以防止其消耗资源过多。这种体系能够明确区分并保证每一个业务流的服务质量，为网络提供最细粒度化的服务质量区分。RSVP 的相关内容请参见“MPLS 配置指导”中的“MPLS TE”。

但是，IntServ 模型对设备的要求很高，当网络中的数据流数量很大时，设备的存储和处理能力会遇到很大的压力。IntServ 模型可扩展性很差，难以在 Internet 核心网络实施。

1.2.3 DiffServ 服务模型

DiffServ 是一个多服务模型，它可以满足不同的 QoS 需求。与 IntServ 不同，它不需要通知网络为每个业务预留资源。区分服务实现简单，扩展性较好。

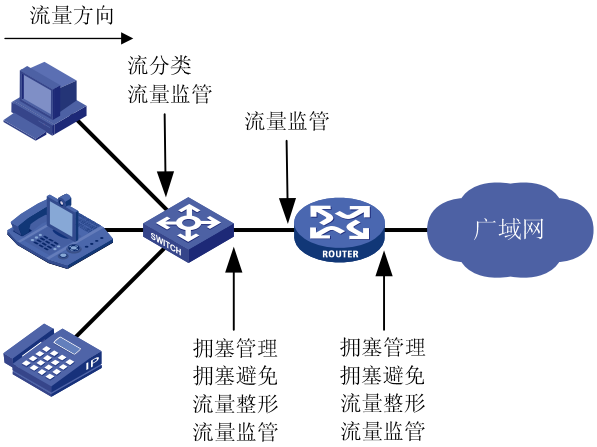
本文提到的技术都是基于 DiffServ 服务模型。

1.3 QoS技术综述

QoS 技术包括流分类、流量监管、流量整形、接口限速、拥塞管理、拥塞避免等。下面对常用的技术进行简单地介绍。

1.3.1 QoS 技术在网络中的位置

图1-1 常用 QoS 技术在网络中的位置



如 图 1-1 所示，流分类、流量监管、流量整形、拥塞管理和拥塞避免主要完成如下功能：

- 流分类：采用一定的规则识别符合某类特征的报文，它是对网络业务进行区分服务的前提和基础。
- 流量监管：对进入或流出设备的特定流量进行监管，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量控制措施，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，通常作用在接口出方向。
- 拥塞管理：当拥塞发生时制定一个资源的调度策略，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，通过调整队列长度来解除网络的过载，通常作用在接口出方向。

1.3.2 QoS 技术在设备中的处理顺序

图1-2 各 QoS 技术在同一网络设备中的处理顺序

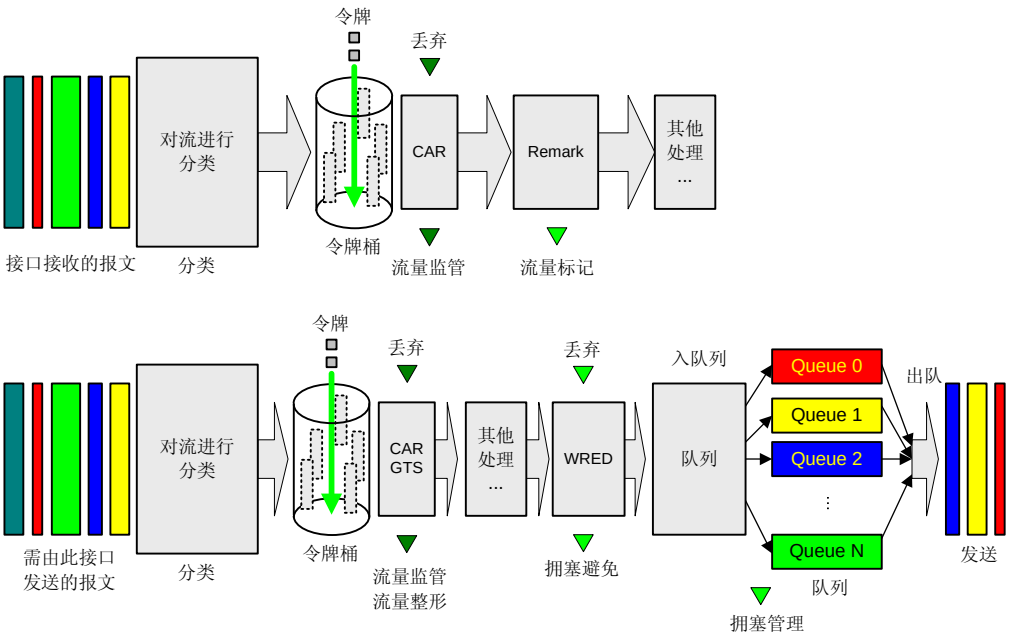


图 1-2 简要描述了各种QoS技术在网络设备中的处理顺序。

(1) 首先通过流分类对各种业务进行识别和区分，它是后续各种动作的基础；

(2) 通过各种动作对特定的业务进行处理。这些动作需要和流分类关联起来才有意义。具体采取何种动作，与所处的阶段以及网络当前的负载状况有关。例如，当报文进入网络时进行流量监管；流出节点之前进行流量整形；拥塞时对队列进行拥塞管理；拥塞加剧时采取拥塞避免措施等。

2 QoS配置方式

2.1 配置方式介绍

QoS 的配置方式分为 QoS 策略配置方式和非 QoS 策略配置方式两种。

有些 QoS 功能只能使用其中一种方式来配置，有些使用两种方式都可以进行配置。在实际应用中，两种配置方式也可以结合起来使用。

2.1.1 非 QoS 策略配置方式

非 QoS 策略配置方式是指不通过 QoS 策略来进行配置。例如，接口限速功能可以通过直接在接口上配置来实现。

2.1.2 QoS 策略配置方式

QoS 策略配置方式是指通过配置 QoS 策略来实现 QoS 功能。

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，灵活地进行 QoS 配置。

1. 类

类的要素包括：类的名称和类的规则。

用户可以通过命令定义一系列的规则来对报文进行分类。

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。

用户可以通过命令在一个流行为中定义多个动作。

3. 策略

策略用来将指定的类和流行为绑定起来，对符合分类条件的报文执行流行为中定义的动作。

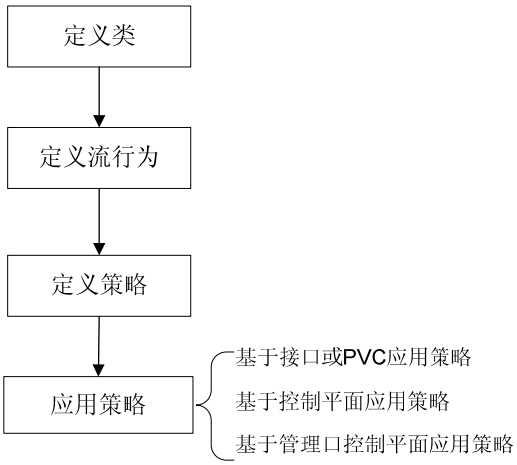
策略的要素包括：策略名称、绑定在一起的类和流行为的名称。

用户可以在一个策略中定义多个类与流行为的绑定关系。

2.2 QoS策略配置方式的步骤

如 图 2-1 所示：

图2-1 QoS 策略配置方式的步骤



2.2.1 定义类

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。

表2-1 定义类

操作	命令	说明
进入系统视图	**system-view**	-
定义一个类，并进入类视图	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	缺省情况下，没有定义类
定义匹配数据包的规则	**if-match** [**not**] *match-criteria*	缺省情况下，没有定义匹配数据包的规则 具体规则请参见QoS命令参考中的命令**if-match**的介绍

2.2.2 定义流行为

定义流行为首先需要创建一个流行为名称，然后可以在此流行为视图下根据需要配置相应的流行为。每个流行为由一组 QoS 动作组成。

表2-2 定义流行为

操作	命令	说明
进入系统视图	**system-view**	-
定义一个流行为，并进入流行为视图	**traffic behavior** *behavior-name*	缺省情况下，没有定义流行为
配置流行为的动作	流行为就是对应符合流分类的报文做出相应的QoS动作，例如流量监管、流量过滤、重标记、流量统计等，具体情况请参见本文相关章节	缺省情况下，没有配置流行为的动作

2.2.3 定义策略

1. 配置父策略

在策略视图下为类指定对应的流行为。以某种匹配规则将流区分为不同的类，再结合不同的流行为就能很灵活的实现各种 QoS 功能。

表2-3 定义策略

操作	命令	说明
进入系统视图	**system-view**	-
定义一个策略，并进入策略视图	**qos policy** *policy-name*	缺省情况下，没有定义策略
为类指定流行为	**classifier** *classifier-name* **behavior** *behavior-name*	缺省情况下，没有为类指定流行为

2. 配置子策略

提示

- 如果子策略中配置了 CBQ，那么父策略中必须配置 GTS，并且配置的父策略 GTS 带宽必须大于等于子策略 CBQ 带宽，否则配置失败。
- 嵌套策略时，如果父策略的 GTS 配置采用百分比形式，则子策略 CBQ 带宽配置必须采用百分比形式，不允许采用绝对值形式；如果父策略的 GTS 配置采用绝对值形式，则子策略 CBQ 带宽配置既可以采用百分比形式，也可以采用绝对值形式。
- 子策略中不允许配置 GTS。

通过在流行为视图下应用子策略，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，还由子策略再次对该类流量进行分类，并执行子策略中定义的行为。

表2-4 配置子策略

操作	命令	说明
进入系统视图	**system-view**	-
定义一个类，并进入类视图	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	缺省情况下，没有定义类
定义匹配数据包的规则	**if-match** [**not**] *match-criteria*	缺省情况下，没有定义匹配数据包的规则 具体规则请参见QoS命令参考中的命令**if-match**的介绍
退回系统视图	**quit**	-
定义一个流行为，并进入流行为视图	**traffic behavior** *behavior-name*	缺省情况下，没有定义流行为
配置子策略	**traffic-policy** *policy-name*	缺省情况下，没有配置嵌套策略

操作	命令	说明
退出流行为视图	**quit**	-
定义一个策略，并进入策略视图	**qos policy** *policy-name*	缺省情况下，没有定义策略
在策略中为类指定采用的流行为	**classifier** *classifier-name* **behavior** *behavior-name*	缺省情况下，没有为类指定流行为

2.2.4 应用策略

QoS 策略支持以下应用方式：

- 基于接口或 PVC 应用 QoS 策略：QoS 策略对通过接口接收或发送的流量生效。
- 基于控制平面应用 QoS 策略：QoS 策略对通过控制平面接收的流量生效。
- 基于管理口控制平面应用 QoS 策略：QoS 策略对通过管理口接收的流量生效。

QoS 策略应用后，用户仍然可以修改 QoS 策略中的流分类规则和流行为，以及二者的对应关系。当流分类规则中匹配的是 ACL 时，允许删除或修改该 ACL（包括向该 ACL 中添加、删除和修改规则）。

1. 基于接口或PVC应用QoS策略

一个策略可以应用于多个接口或 PVC。接口或 PVC 的每个方向（出和入两个方向）只能应用一个策略。

如果 QoS 策略应用在接口或 PVC 的出方向，则 QoS 策略对本地协议报文不起作用。本地协议报文是设备内部发起的某些报文，它是维持设备正常运行的重要协议报文。为了确保这些报文能够被不受影响的发送出去，即便在接口或 PVC 的出方向应用了 QoS 策略，本地协议报文也不会受到 QoS 策略的限制，从而降低了因配置 QoS 而误将这些报文丢弃或进行其他处理的风险。一些常见的本地协议报文如下：链路维护报文、IS-IS、OSPF、RIP、BGP、LDP、RSVP、SSH 等。

表2-5 在接口或 PVC 上应用策略

操作		命令	说明
进入系统视图		**system-view**	-
进入接口视图或PVC视图	进入接口视图	**interface** *interface-type interface-number*	二者选其一 进入接口视图后，下面进行的配置只在当前接口生效；进入PVC视图后，下面进行的配置只在当前PVC生效
	进入PVC视图	**interface atm** *interface-number*	
		pvc *vpi/vci*	
在接口或PVC上应用QoS策略		**qos apply policy** *policy-name* { **inbound** | **outbound** }	缺省情况下，没有在接口或PVC上应用QoS策略

2. 基于控制平面应用QoS策略

提示

当某个单板资源不足导致控制平面应用 QoS 策略失败时，用户可以执行 **undo qos apply policy** 命令进行手工删除。

设备上存在数据平面和控制平面：

- 数据平面（Data Plane）：是指对报文进行收发、交换的处理单元，它的主要工作是转发报文。在设备上，与之相对应的核心物理实体就是各种专用转发芯片，它们有极高的处理速度和很强的数据吞吐能力。
- 控制平面（Control Plane）：是指运行大部分路由交换协议进程的处理单元，它的主要工作是进行协议报文的解析和协议的计算。在设备上，与之相对应的核心物理实体就是 CPU，它具备灵活的报文处理能力，但数据吞吐能力有限。

数据平面接收到无法识别或处理的报文会送到控制平面进行进一步处理。如果上送控制平面的报文速率超过了控制平面的处理能力，那么上送控制平面的报文会得不到正确转发或及时处理，从而影响协议的正常运行。

为了解决此问题，用户可以把 QoS 策略应用在控制平面上，通过对上送控制平面的报文进行过滤、限速等 QoS 处理，达到保护控制平面正常报文的收发、维护控制平面正常处理状态的目的。

缺省情况下，设备会在控制平面上应用预定义的 QoS 策略，并默认生效。预定义的 QoS 策略中通过协议类型或者协议组类型来标识各种上送控制平面的报文类型，用户也可以在流分类视图下通过 **if-match** 命令引用这些协议类型或者协议组类型来进行报文分类，然后根据需要为这些报文重新配置流行为。系统预定义的 QoS 策略信息可以通过 **display qos policy control-plane pre-defined** 命令查看。

表2-6 应用控制平面策略

操作	命令	说明
进入系统视图	**system-view**	-
进入控制平面视图（MSR 2600/MSR 3600）	**control-plane**	-
进入控制平面视图（MSR 5600）	**control-plane slot** *slot-number*	-
在控制平面上应用QoS策略	**qos apply policy** *policy-name* **inbound**	缺省情况下，没有在控制平面上应用QoS策略

3. 基于管理口控制平面应用QoS策略

MSR 系列路由器各款型对于本节所描述的特性的支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR 2600	基于管理口控制平面应用QoS策略	不支持
MSR 3600		不支持

型号	特性	描述
MSR 5600		支持

管理口控制平面仅针对管理口上送给控制平面的报文。

如果管理口上送给控制平面的报文速率超过其处理能力，报文会得不到正确转发或及时处理，从而影响协议的正常运行。

为了解决此问题，用户可以把 QoS 策略应用在管理口控制平面上，通过对管理口上送给控制平面的报文进行 QoS 限速处理，达到保护管理口正常报文的收发、维护管理口正常处理状态的目的。

缺省情况下，会在管理口上应用预定义的 QoS 限速策略，并默认生效。预定义的 QoS 策略中通过协议类型或者协议组类型来标识各种上送管理口的报文类型，用户也可以在流分类视图下通过 **if-match** 命令引用这些协议类型或者协议组类型来进行报文分类，然后根据需要为这些报文重新配置流行为。系统预定义的 QoS 策略信息可以通过 **display qos policy control-plane management pre-defined** 命令查看。

表2-7 应用管理口控制平面策略

操作	命令	说明
进入系统视图	**system-view**	-
进入管理口控制平面视图	**control-plane management**	-
在管理口控制平面上应用QoS策略	**qos apply policy** *policy-name* **inbound**	缺省情况下，没有在管理口控制平面上应用QoS策略

2.2.5 配置接口流速统计时间

提示

- ATM PVC 的流速统计时间采用所在 ATM 接口上设置的统计时间。
- 子接口的流速统计时间采用主接口上设置的统计时间。

我们可以统计经过 QoS 策略流分类后每类报文的发送和丢弃速率。假设流速统计时间为 t（t 默认为 5 分钟），则系统将统计最近 t 时间内每类报文发送和丢弃的平均速率，且每 t/5 分钟刷新一次统计速率。流速统计的结果可以通过命令 **display qos policy interface** 查看。

表2-8 配置接口流速统计时间

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置接口流速统计时间	**qos flow-interval** *interval*	缺省情况下，接口流速统计时间为5分钟

2.2.6 QoS 策略显示和维护

在任意视图下执行 **display** 命令可以显示 QoS 策略的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 QoS 策略的统计信息。

表2-9 QoS 策略显示和维护

操作	命令
显示类的配置信息（MSR 2600/MSR 3600）	**display traffic classifier** { **system-defined** | **user-defined** } [*classifier-name*]
显示类的配置信息（MSR 5600）	**display traffic classifier** { **system-defined** | **user-defined** } [*classifier-name*] [**slot** *slot-number*]
显示流行为的配置信息（MSR 2600/MSR 3600）	**display traffic behavior** { **system-defined** | **user-defined** } [*behavior-name*]
显示流行为的配置信息（MSR 5600）	**display traffic behavior** { **system-defined** | **user-defined** } [*behavior-name*] [**slot** *slot-number*]
显示QoS策略的配置信息（MSR 2600/MSR 3600）	**display qos policy** { **system-defined** | **user-defined** } [*policy-name* [**classifier** *classifier-name*]]
显示QoS策略的配置信息（MSR 5600）	**display qos policy** { **system-defined** | **user-defined** } [*policy-name* [**classifier** *classifier-name*]] [**slot** *slot-number*]
显示接口上QoS策略的配置信息和运行情况（MSR 2600/MSR 3600）	**display qos policy interface** [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]] [**inbound** | **outbound**]
显示接口上QoS策略的配置信息和运行情况（MSR 5600）	**display qos policy interface** [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]] [**slot** *slot-number*] [**inbound** | **outbound**]
显示基于控制平面应用QoS策略的信息（MSR 2600/MSR 3600）	**display qos policy control-plane**
显示基于控制平面应用QoS策略的信息（MSR 5600）	**display qos policy control-plane slot** *slot-number*
显示基于管理口控制平面应用QoS策略的信息（MSR 5600）	**display qos policy control-plane management**
显示系统预定义的控制平面应用QoS策略的信息（MSR 2600/MSR 3600）	**display qos policy control-plane pre-defined**
显示系统预定义的控制平面应用QoS策略的信息（MSR 5600）	**display qos policy control-plane pre-defined** [**slot** *slot-number*]
显示系统预定义的管理口控制平面应用QoS策略的信息（MSR 5600）	**display qos policy control-plane management pre-defined**
清除控制平面应用QoS策略的统计信息（MSR 2600/MSR 3600）	**reset qos policy control-plane**
清除控制平面应用QoS策略的统计信息（MSR 5600）	**reset qos policy control-plane slot** *slot-number*
清除管理口控制平面应用QoS策略的统计信息（MSR 5600）	**reset qos policy control-plane management**

3 优先级映射

3.1 优先级映射简介

报文在进入设备以后，设备会根据映射规则分配或修改报文的各种优先级的值，为队列调度和拥塞控制服务。

优先级映射功能通过报文所携带的优先级字段来映射其他优先级字段值，就可以获得决定报文调度能力的各种优先级字段，从而为全面有效的控制报文的转发调度等级提供依据。

3.1.1 优先级介绍

优先级用于标识报文传输的优先程度，可以分为两类：报文携带优先级和设备调度优先级。

报文携带优先级包括：802.1p优先级、DSCP优先级、IP优先级、EXP优先级等。这些优先级都是根据公认的标准和协议生成，体现了报文自身的优先等级。相关介绍请参见 11.3 附录 C 各种优先级介绍。

设备调度优先级是指报文在设备内转发时所使用的优先级，只对当前设备自身有效。设备调度优先级包括以下几种：

- 本地优先级（LP）：设备为报文分配的一种具有本地意义的优先级，每个本地优先级对应一个队列，本地优先级值越大的报文，进入的队列优先级越高，从而能够获得优先的调度。
- 用户优先级（UP）：设备对于进入的流量，会自动获取报文的优先级作为后续转发调度的参数，这种报文优先级称为用户优先级。对于不同类型的报文，用户优先级所代表的优先级字段不同。对于二层报文，用户优先级取自 802.1p 优先级；对于三层报文，用户优先级取自 IP 优先级；对于 MPLS 报文，用户优先级取自 EXP。

3.1.2 优先级映射表

设备提供了多张优先级映射表，分别对应不同的优先级映射关系。

通常情况下，设备可以通过查找缺省优先级映射表（11.2 附录 B 缺省优先级映射表）来为报文分配相应的优先级。如果缺省优先级映射表无法满足用户需求，可以根据实际情况对映射表进行修改。

3.2 优先级映射配置任务简介

常用的方式有两种：配置优先级信任模式和配置端口优先级。

如果配置了优先级信任模式，即表示设备信任所接收报文的优先级，会自动解析报文的优先级或者标志位，然后按照映射表映射到报文的优先级参数。

如果没有配置优先级信任模式，并且配置了端口优先级值，则表明设备不信任所接收报文的优先级，而是使用端口优先级，按照映射表映射到报文的优先级参数。

表3-1 优先级映射配置任务简介

配置任务	说明	详细配置
配置不带颜色的优先级映射表	可选	3.3.1

配置任务	说明	详细配置
配置优先级信任模式	二者必选其一	3.3.2
配置端口优先级		3.3.3

3.3 配置优先级映射

3.3.1 配置不带颜色的优先级映射表

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。

表3-2 优先级映射表

优先级映射	描述
dot1p-lp	802.1p优先级到本地优先级映射表
dscp-lp	DSCP到本地优先级映射表

表3-3 配置不带颜色的优先级映射表

操作	命令	说明
进入系统视图	**system-view**	-
进入指定的优先级映射表视图	**qos map-table** { **dot1p-lp** | **dscp-lp** }	用户根据需要进入相应的优先级映射表视图
配置指定优先级映射表的映射关系	**import** *import-value-list* **export** *export-value*	缺省情况下，优先级映射表的映射关系请参见11.2 附录 B 缺省优先级映射表（不带颜色） 新配置的映射关系将覆盖原有映射关系

3.3.2 配置优先级信任模式

说明

本节特性仅在路由器安装了二层以太网交换模块时支持。接口模块的详细介绍请参见《H3C MSR系列路由器接口模块手册》。

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，可以通过配置优先级信任模式的方式来实现。

在配置接口上的优先级模式时，用户可以选择下列信任模式：

- **dot1p**：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。

表3-4 配置优先级信任模式

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置优先级信任模式	**qos trust** { **dot1p** | **dscp** }	缺省情况下，配置优先级信任模式

3.3.3 配置端口优先级

按照接收端口的端口优先级，设备通过一一映射为报文分配相应的优先级。

表3-5 配置端口优先级

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置端口优先级	**qos priority** *priority-value*	端口优先级的缺省值为0

3.4 优先级映射显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后优先级映射的运行情况，通过查看显示信息验证配置的效果。

表3-6 优先级映射显示和维护

操作	命令
显示指定优先级映射表配置情况	**display qos map-table** [**dot1p-lp** | **dscp-lp**]
显示端口优先级信任模式信息	**display qos trust interface** [*interface-type interface-number*]

3.5 优先级映射典型配置举例

3.5.1 优先级信任模式和端口优先级配置举例

1. 组网需求

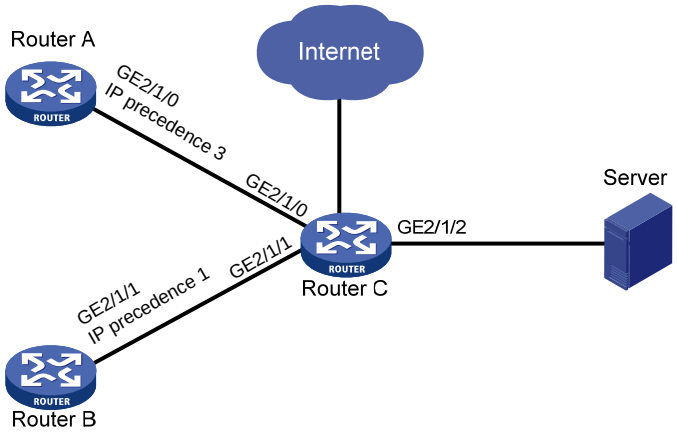
Router A 和 Router B 通过 Router C 实现互连。网络环境描述如下：

- Router A 通过端口 GigabitEthernet2/1/0 接入 Router C，向 Router C 发送 IP 优先级值为 3 的报文；
- Router B 通过端口 GigabitEthernet2/1/1 接入 Router C，向 Router C 发送 IP 优先级值为 1 的报文。

要求通过配置实现如下需求：如果 Router C 在接口 GigabitEthernet2/1/2 的出方向发生拥塞，则优先处理 Router A 发出的报文（优先让 Router A 访问 Server）。

2. 组网图

图3-1 优先级信任模式和端口优先级配置组网图



3. 配置步骤

在接口 GigabitEthernet2/1/0 和 GigabitEthernet2/1/1 上分别配置端口优先级，GigabitEthernet2/1/0 上配置的端口优先级值要高于 GigabitEthernet2/1/1 上配置的端口优先级值。

```
<RouterC> system-view
[RouterC] interface gigabitethernet 2/1/0
[RouterC-GigabitEthernet2/1/0] qos priority 3
[RouterC-GigabitEthernet2/1/0] quit
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] qos priority 1
[RouterC-GigabitEthernet2/1/1] quit
```

3.5.2 优先级映射表和重标记配置举例

1. 组网需求

公司企业网通过 Router 实现各部门之间的互连。网络环境描述如下：

- 市场部门通过端口 GigabitEthernet2/1/0 接入 Router，标记市场部门发出的报文的 802.1p 优先级为 3；
- 研发部门通过端口 GigabitEthernet2/1/1 接入 Router，标记研发部门发出的报文的 802.1p 优先级为 4；
- 管理部门通过端口 GigabitEthernet2/1/2 接入 Router，标记管理部门发出的报文的 802.1p 优先级为 5。

实现如下需求：

访问公共服务器的时候，研发部门 > 管理部门 > 市场部门。

- 通过优先级映射将研发部门发出的报文放入出队列 6 中，优先进行处理；
- 通过优先级映射将管理部门发出的报文放入出队列 4 中，次优先进行处理；

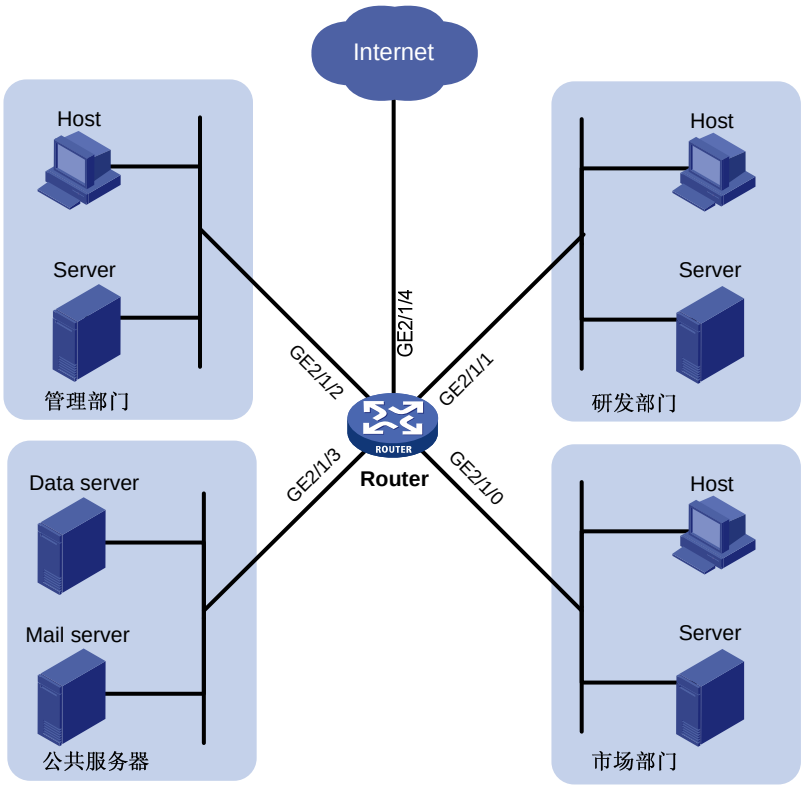
- 通过优先级映射将市场部门发出的报文放入出队列 2 中，最后进行处理。

访问 Internet 的时候，管理部门 > 市场部门 > 研发部门。

- 管理部门优先进行处理；
- 重标记市场部门发出的报文的本地优先级为 3，次优先进行处理；
- 重标记研发部门发出的报文的本地优先级为 2，最后进行处理。

2. 组网图

图3-2 优先级映射表和重标记配置组网图



3. 配置步骤

(1) 配置端口的端口优先级

配置端口 GigabitEthernet2/1/0 的端口优先级为 3。

```
<Router> system-view
[Router] interface gigabitethernet 2/1/0
[Router-GigabitEthernet2/1/0] qos priority 3
[Router-GigabitEthernet2/1/0] quit
```

配置端口 GigabitEthernet2/1/1 的端口优先级为 4。

```
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] qos priority 4
[Router-GigabitEthernet2/1/1] quit
```

配置端口 GigabitEthernet2/1/2 的端口优先级为 5。

```
[Router] interface gigabitethernet 2/1/2
[Router-GigabitEthernet2/1/2] qos priority 5
[Router-GigabitEthernet2/1/2] quit
```

(2) 配置优先级映射表

配置 802.1p 优先级到本地优先级映射表，将 802.1p 优先级 3、4、5 对应的本地优先级配置为 2、6、4。保证访问服务器的优先级为研发部门（6）>管理部门（4）>市场部门（2）。

```
[Router] qos map-table dot1p-lp
[Router-maptbl-dot1p-lp] import 3 export 2
[Router-maptbl-dot1p-lp] import 4 export 6
[Router-maptbl-dot1p-lp] import 5 export 4
[Router-maptbl-dot1p-lp] quit
```

(3) 配置重标记

将本地优先级 6、2 重标记为 2、3，本地优先级 4 保持不变。保证访问 Internet 的优先级为管理部门（4）>市场部门（3）>研发部门（2）。

```
[Router] traffic classifier rd
[Router-classifier-rd] if-match local-precedence 6
[Router-classifier-rd] quit
[Router] traffic classifier market
[Router-classifier-market] if-match local-precedence 2
[Router-classifier-market] quit
[Router] traffic behavior rd
[Router-behavior-rd] remark local-precedence 2
[Router-behavior-rd] quit
[Router] traffic behavior market
[Router-behavior-market] remark local-precedence 3
[Router-behavior-market] quit
[Router] qos policy policy1
[Router-qospolicy-policy1] classifier rd behavior rd
[Router-qospolicy-policy1] classifier market behavior market
[Router-qospolicy-policy1] quit
[Router] interface gigabitethernet 2/1/4
[Router-GigabitEthernet2/1/4] qos apply policy policy1 outbound
```

4 流量监管、流量整形和接口限速

4.1 流量监管、流量整形和接口限速简介

如果不限制用户发送的流量，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、流量整形和接口限速可以实现流量的速率限制功能，而要实现此功能就必须对通过设备的流量进行度量。一般采用令牌桶（Token Bucket）对流量进行度量。

4.1.1 流量评估与令牌桶

1. 令牌桶的特点

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。

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，称流量遵守或符合这个规格，否则称为不符合或超标。

评估流量时令牌桶的参数包括：

- 平均速率：向桶中放置令牌的速率，即允许的流的平均速度。通常配置为 CIR。
- 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。通常配置为 CBS，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，此时要从桶中取走满足报文的转发的令牌；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，可以配置两个令牌桶（分别称为 C 桶和 E 桶）。例如流量监管中有四个参数：

- CIR：表示向 C 桶中投放令牌的速率，即 C 桶允许传输或转发报文的平均速率；
- CBS：表示 C 桶的容量，即 C 桶瞬间能够通过的承诺突发流量；
- PIR：表示向 E 桶中投放令牌的速率，即 E 桶允许传输或转发报文的最大速率；
- EBS：表示 E 桶的容量，即 E 桶瞬间能够通过的超出突发流量。

CBS 和 EBS 是由两个不同的令牌桶承载的。每次评估时，依据下面的情况，可以分别实施不同的流控策略：

- 如果 C 桶有足够的令牌，报文被标记为 green，即绿色报文；
- 如果 C 桶令牌不足，但 E 桶有足够的令牌，报文被标记为 yellow，即黄色报文；
- 如果 C 桶和 E 桶都没有足够的令牌，报文被标记为 red，即红色报文。

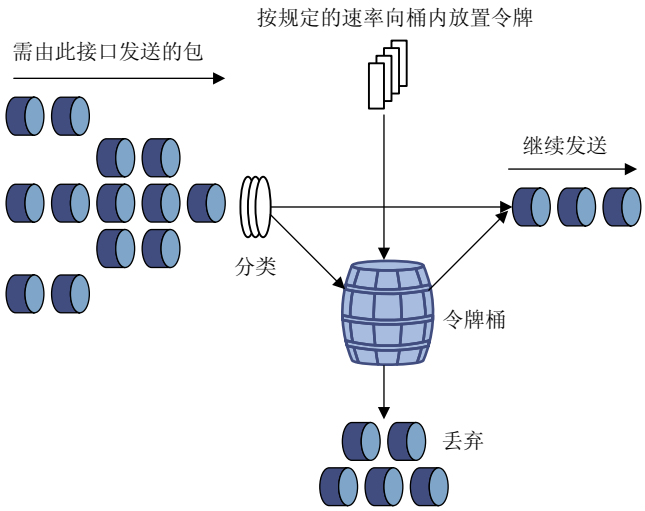
4.1.2 流量监管

说明

流量监管支持入和出两个方向，为了方便描述，下文以出方向为例。

流量监管就是对流量进行控制，通过监督进入网络的流量速率，对超出部分的流量进行“惩罚”，使进入的流量被限制在一个合理的范围之内，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，或重新配置报文的优先级。

图4-1 TP 示意图



流量监管广泛的用于监管进入 Internet 服务提供商 ISP 的网络流量。流量监管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“符合”的报文，将其优先级进行重标记后再进行转发。
- 改变优先级并进入下一级监管：比如对评估结果为“符合”的报文，将其优先级进行重标记后再进入下一级的监管。
- 进入下一级的监管：流量监管可以进行分级，每级关注和监管更具体的目标。

4.1.3 流量整形

说明

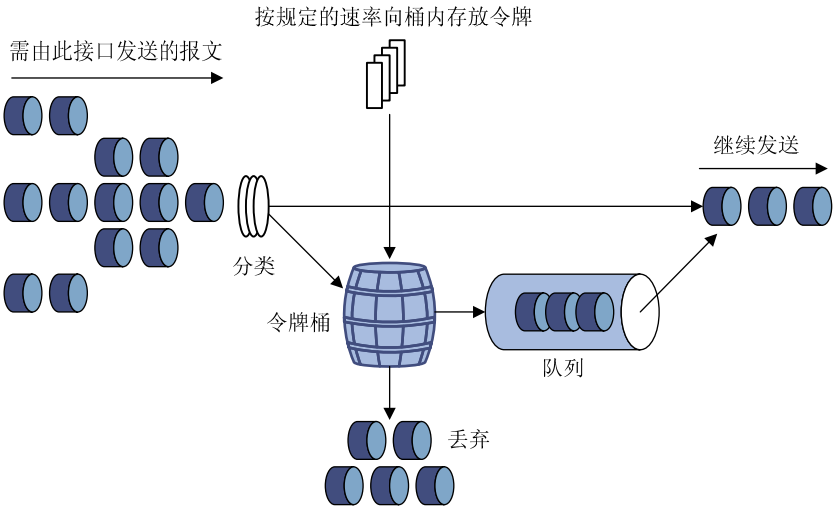
流量整形目前只支持出方向。

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

流量整形与流量监管的主要区别在于：

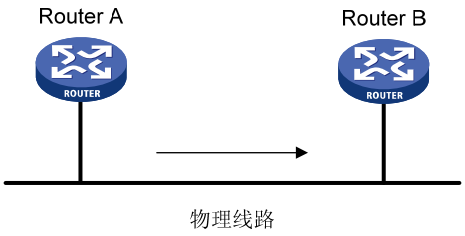
- 流量整形对流量监管中需要丢弃的报文进行缓存——通常是将它们放入缓冲区或队列内，如图 4-2 所示。当令牌桶有足够的令牌时，再均匀的向外发送这些被缓存的报文。
- 流量整形可能会增加延迟，而流量监管几乎不引入额外的延迟。

图4-2 流量整形示意图



例如，在 图 4-3 所示的应用中，设备Router A向Router B发送报文。Router B要对Router A发送来的报文进行流量监管，对超出规格的流量直接丢弃。

图4-3 流量整形的应用



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

4.1.4 接口限速

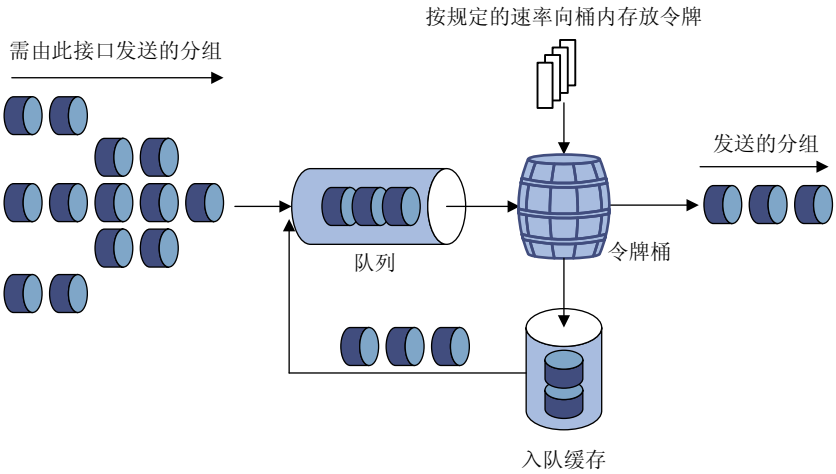
说明

接口限速支持入/出两个方向，为了方便描述，下文以出方向为例。

利用接口限速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。

接口限速也是采用令牌桶进行流量控制。如果在设备的某个接口上配置了接口限速，所有经由该接口发送的报文首先要经过接口限速的令牌桶进行处理。如果令牌桶中有足够的令牌，则报文可以发送；否则，报文将进入 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4-4 接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。

与流量监管相比，物理接口限速能够限制在物理接口上通过的所有报文。当用户只要求对所有报文限速时，使用物理接口限速比较简单。

4.2 配置流量监管

流量监管的配置有两种方式：QoS 策略配置方式和非 QoS 策略配置方式。

如果接口上同时采用了 QoS 策略配置方式和非 QoS 策略配置方式配置了流量监管，那么只有前者会生效。

4.2.1 QoS 策略配置方式

表4-1 配置流量监管（QoS 策略配置方式）

操作	命令	说明
进入系统视图	**system-view**	-
定义一个类，并进入类视图	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	缺省情况下，没有定义类
定义匹配数据包的规则	**if-match** [**not**] *match-criteria*	缺省情况下，没有定义匹配数据包的规则 具体规则请参见QoS命令参考中的命令**if-match**的介绍

操作		命令	说明
退回系统视图		**quit**	-
定义一个流行为，并进入流行为视图		**traffic behavior** *behavior-name*	缺省情况下，没有定义流行为
配置流量监管动作		**car cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**pir** *peak-information-rate*] [**green** *action* | **red** *action* | **yellow** *action*] *	缺省情况下，没有配置流量监管动作
退回系统视图		**quit**	-
定义一个策略，并进入策略视图		**qos policy** *policy-name*	缺省情况下，没有定义策略
在策略中为类指定采用的流行为		**classifier** *classifier-name* **behavior** *behavior-name*	缺省情况下，没有为类指定流行为
退回系统视图		**quit**	-
应用QoS策略	基于接口或PVC	2.2.4 1. 基于接口或PVC应用QoS策略	三者选其一 缺省情况下，没有应用QoS策略
	基于控制平面	2.2.4 2. 基于控制平面应用QoS策略	
	基于管理口控制平面	2.2.4 3. 基于管理口控制平面应用QoS策略	
（可选）显示流量监管的相关配置信息		**display qos policy user-defined** [*policy-name*]	**display**命令可以在任意视图下执行

4.2.2 非 QoS 策略配置方式

1. 基于CAR列表的流量监管配置

表4-2 基于 CAR 列表的流量监管配置

操作	命令	说明
进入系统视图	**system-view**	-
配置CAR列表	**qos carl** *carl-index* { **dscp** *dscp-list* | **mac** *mac-address* | **mpls-exp** *mpls-exp-value* | **precedence** *precedence-value* | { **destination-ip-address** | **source-ip-address** } { **range** *start-ip-address* **to** *end-ip-address* | **subnet** *ip-address mask-length* } [**per-address** [**shared-bandwidth**]] }	缺省情况下，没有配置CAR列表
进入接口视图	**interface** *interface-type interface-number*	-
在接口应用基于CAR列表的CAR策略	**qos car** { **inbound** | **outbound** } **carl** *carl-index* **cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**pir** *peak-information-rate*] [**green** *action* | **red** *action* | **yellow** *action*] *	缺省情况下，接口上没有配置CAR

2. 基于ACL的流量监管配置

表4-3 基于 ACL 的流量监管配置

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
在接口应用基于ACL规则的CAR策略	**qos car** { **inbound** | **outbound** } **acl** [**ipv6**] *acl-number* **cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**pir** *peak-information-rate*] [**green** *action* | **red** *action* | **yellow** *action*] *	缺省情况下，接口上没有配置CAR

3. 适配所有流的流量监管配置

表4-4 适配所有流的流量监管配置

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
在接口应用CAR策略	**qos car** { **inbound** | **outbound** } **any cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**pir** *peak-information-rate*] [**green** *action* | **red** *action* | **yellow** *action*] *	缺省情况下，接口上没有配置CAR

4.3 配置流量整形

4.3.1 QoS 策略配置方式

表4-5 配置流量整形（QoS 策略配置方式）

操作	命令	说明
进入系统视图	**system-view**	-
定义一个类，并进入类视图	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	缺省情况下，没有定义类
定义匹配数据包的规则	**if-match** [**not**] *match-criteria*	缺省情况下，没有定义匹配数据包的规则 具体规则请参见QoS命令参考中的命令**if-match**的介绍
退回系统视图	**quit**	-

操作		命令	说明
定义一个流行为，并进入流行为视图		**traffic behavior** *behavior-name*	缺省情况下，没有定义流行为
配置流量整形动作		**gts cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**queue-length** *queue-length*] **gts percent cir** *cir-percent* [**cbs** *cbs-time* [**ebs** *ebs-time*]] [**queue-length** *queue-length*]	缺省情况下，没有配置流量整形动作
退回系统视图		**quit**	-
定义一个策略，并进入策略视图		**qos policy** *policy-name*	缺省情况下，没有定义策略
在策略中为类指定采用的流行为		**classifier** *classifier-name* **behavior** *behavior-name*	缺省情况下，没有为类指定流行为
退回系统视图		**quit**	-
应用QoS策略	基于接口或PVC	2.2.4 1. 基于接口或PVC应用QoS策略	二者选其一 缺省情况下，没有应用QoS策略
	基于控制平面	2.2.4 2. 基于控制平面应用QoS策略	
（可选）显示流量监管的相关配置信息		**display qos policy user-defined** [*policy-name*]	**display**命令可以在任意视图下执行

4.3.2 非 QoS 策略配置方式

非 QoS 策略流量整形配置分为以下几种：

- 基于 ACL 的流量整形配置：为匹配某一 ACL 的流设置整形参数，使用不同的 ACL 可以为不同的流设置流量整形参数。
- 适配所有流的流量整形配置：为所有的流设置流量整形参数。

1. 基于ACL的流量整形配置

表4-6 基于 ACL 的流量整形配置

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
在接口配置流量整形	**qos gts acl** [**ipv6**] *acl-number* **cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**queue-length** *queue-length*]	缺省情况下，接口上没有配置流量整形

2. 适配所有流的流量整形配置

表4-7 适配所有流的流量整形配置

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
在接口配置流量整形	**qos gts any cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**queue-length** *queue-length*]	缺省情况下，接口上没有配置流量整形

4.4 配置接口限速

配置接口限速就是限制接口向外发送数据或者接收数据的速率。

表4-8 接口限速配置过程

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置接口限速	**qos lr** { **inbound** | **outbound** } **cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]]	缺省情况下，接口上没有配置接口限速

4.5 流量监管、流量整形和接口限速显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后流量监管、流量整形和接口限速的运行情况，通过查看显示信息验证配置的效果。

表4-9 流量监管、流量整形和接口限速显示和维护

操作	命令
显示接口的流量监管配置情况和统计信息	**display qos car interface** [*interface-type interface-number*]
显示CAR列表	**display qos carl** [*carl-index*]
显示流量监管的相关配置信息	**display qos policy user-defined** [*policy-name*]
显示接口的流量整形配置情况和统计信息	**display qos gts interface** [*interface-type interface-number*]
显示接口的接口限速配置情况和统计信息	**display qos lr interface** [*interface-type interface-number*]

4.6 流量监管与流量整形典型配置举例

4.6.1 流量监管与流量整形典型配置举例

1. 配置需求

- 设备 Router A 通过接口 GigabitEthernet2/1/2 和设备 Router B 的接口 GigabitEthernet2/1/0 互连
- Server、Host A、Host B 可经由 Router A 和 Router B 访问 Internet
- Server、Host A 与 Router A 的 GigabitEthernet2/1/0 接口在同一网段
- Host B 与 Router A 的 GigabitEthernet2/1/1 接口在同一网段

要求在设备 Router A 上对接口 GigabitEthernet2/1/0 接收到的源自 Server 和 Host A 的报文流分别实施流量控制如下：

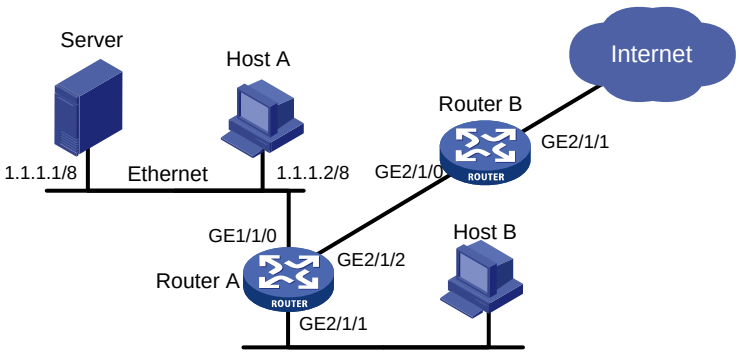
- 来自 Server 的报文流量约束为 54kbps，流量小于 54kbps 时可以正常发送，流量超过 54kbps 时则将违规报文的优先级设置为 0 后进行发送；
- 来自 Host A 的报文流量约束为 8kbps，流量小于 8kbps 时可以正常发送，流量超过 8kbps 时则丢弃违规报文；

对设备 Router B 的 GigabitEthernet2/1/0 和 GigabitEthernet2/1/1 接口收发报文有如下要求：

- Router B 的 GigabitEthernet2/1/0 接口接收报文的总流量限制为 500kbps，如果超过流量限制则将违规报文丢弃；
- 经由 Router B 的 GigabitEthernet2/1/1 接口进入 Internet 的报文流量限制为 1000kbps，如果超过流量限制则将违规报文丢弃。

2. 组网图

图4-5 流量监管、流量整形配置组网图



3. 配置步骤

(1) 配置设备 Router A

在 GigabitEthernet2/1/2 接口上对发送的报文进行流量整形（对超过 500kbps 的报文流进行整形），以降低在 Router B 接口 GigabitEthernet2/1/0 处的丢包率。

```
<RouterA> system-view
[RouterA] interface gigabitethernet 2/1/2
[RouterA-GigabitEthernet2/1/2] qos gts any cir 500
```

```
[RouterA-GigabitEthernet2/1/2] quit
```

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

```
[RouterA] acl number 2001
[RouterA-acl-basic-2001] rule permit source 1.1.1.1 0
[RouterA-acl-basic-2001] quit
[RouterA] acl number 2002
[RouterA-acl-basic-2002] rule permit source 1.1.1.2 0
[RouterA-acl-basic-2002] quit
```

在 GigabitEthernet2/1/0 接口上对接收到的不同报文流进行相应流量控制。

```
[RouterA] interface gigabitethernet 2/1/0
[RouterA-GigabitEthernet2/1/0] qos car inbound acl 2001 cir 54 cbs 4000 ebs 0 green pass red remark-prec-pass 0
[RouterA-GigabitEthernet2/1/0] qos car inbound acl 2002 cir 8 cbs 1875 ebs 0 green pass red discard
[RouterA-GigabitEthernet2/1/0] quit
```

(2) 配置设备 Router B

在 GigabitEthernet2/1/0 接口上对接收的报文进行流量控制，报文流量不能超过 500kbps，如果超过流量限制则将违规报文丢弃。

```
<RouterB> system-view
[RouterB] interface gigabitethernet 2/1/0
[RouterB-GigabitEthernet2/1/0] qos car inbound any cir 500 cbs 32000 ebs 0 green pass red discard
[RouterB-GigabitEthernet2/1/0] quit
```

在 GigabitEthernet2/1/1 接口上对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。

```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] qos car outbound any cir 1000 cbs 65000 ebs 0 green pass red discard
```

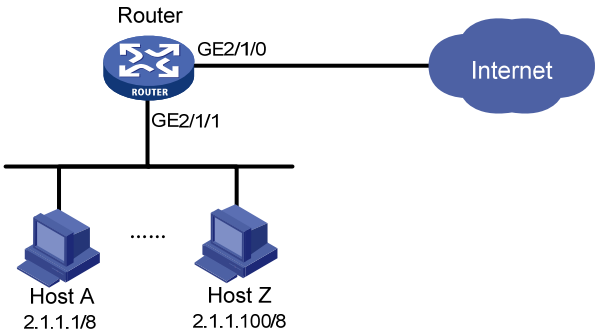
4.6.2 IP 限速典型配置举例

1. 配置需求

要求在设备 Router 上对接口 GigabitEthernet2/1/1 接收到的报文流进行限速：对 HostA～HostZ（源地址属于 IP 地址段 2.1.1.1～2.1.1.100）进行 IP 限速，逐 IP 地址流量限速 5kbps，网段内各 IP 地址的流量共享剩余带宽。

2. 组网图

图4-6 IP 限速配置组网图



3. 配置步骤

在接口 GigabitEthernet2/1/1 上对源地址属于 IP 地址段 2.1.1.1～2.1.1.100 内所有 PC 进行限速，网段内各 IP 地址的流量共享剩余带宽。

```
<Router> system-view
[Router] qos carl 1 source-ip-address range 2.1.1.1 to 2.1.1.100 per-address shared-bandwidth
[Router] interface gigabitethernet 2/1/1
[Router-GigabitEthernet2/1/1] qos car inbound carl 1 cir 500 cbs 1875 ebs 0 green pass red discard
[Router-GigabitEthernet2/1/1] quit
```

5 拥塞管理

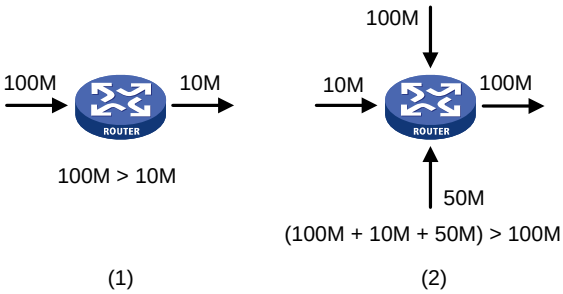
5.1 拥塞管理简介

5.1.1 拥塞的产生、影响和对策

所谓拥塞，是指当前供给资源相对于正常转发处理需要资源的不足，从而导致服务质量下降的一种现象。

在复杂的Internet分组交换环境下，拥塞极为常见。以 图 5-1 中的两种情况为例：

图5-1 流量拥塞示意图



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，可能会引起报文重传，从而导致更多的拥塞产生。
- 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。

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。

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，以决定报文转发的处理次序。

5.1.2 拥塞管理策略

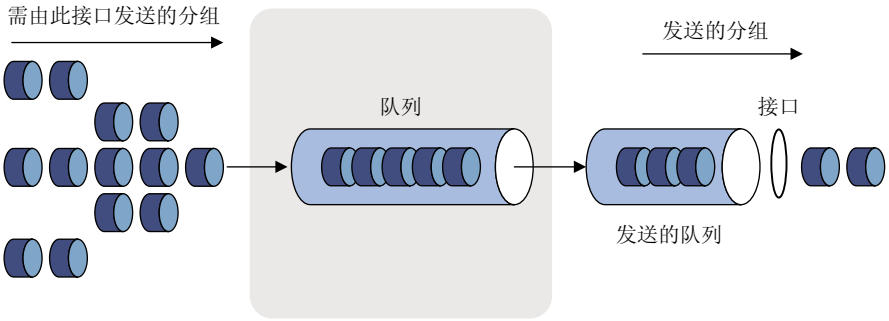
对于拥塞管理，一般采用队列技术，使用一个队列算法对流量进行分类，之后用某种优先级别算法将这些流量发送出去。每种队列算法都是用以解决特定的网络流量问题，并对带宽资源的分配、延迟、抖动等有着十分重要的影响。

拥塞管理的处理包括队列的创建、报文的分类、将报文送入不同的队列、队列调度等。

下面介绍几种常用的队列。

1. FIFO队列

图5-2 先入先出队列示意图



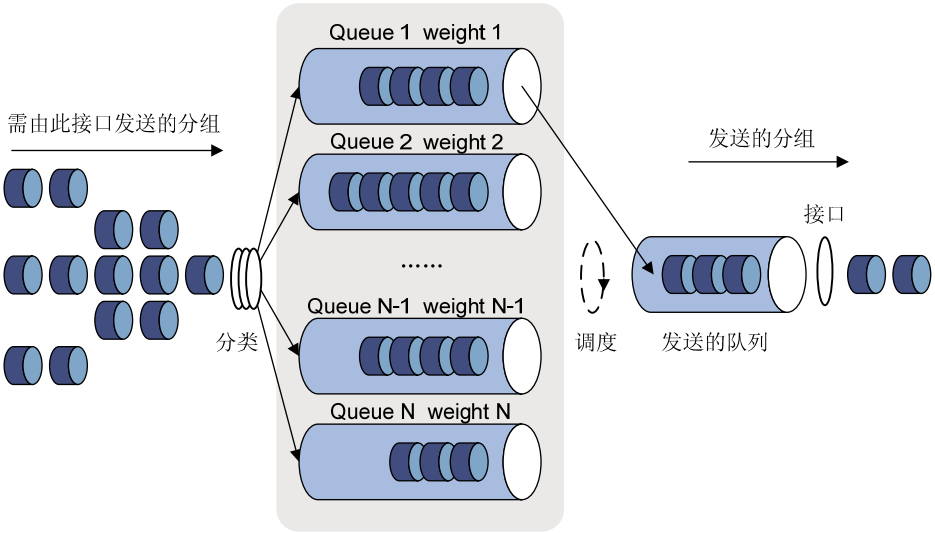
如 图 5-2 所示，FIFO按照时间到达的先后决定分组的转发次序，先进的先出，后进的后出，不需要进行流分类和队列调度，FIFO关心的只是队列的长度，队列的长度对延迟和丢包率的影响。用户的业务流在某个设备能够获得的资源取决于分组的到达时机及当时的负载情况。Best-Effort报文转发方式采用的就是FIFO的排队策略。

如果设备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。所以还需要配置一些其他的队列调度机制与 FIFO 配合对流量进行调度和拥塞控制。

每个队列内部报文的发送次序缺省是 FIFO。

2. WFQ队列

图5-3 WFQ 队列示意图



在介绍加权公平队列前，先要理解 FQ 队列。FQ 队列是为了公平地分享网络资源，尽可能使所有流的延迟和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：

- 不同的队列获得公平的调度机会，从总体上均衡各个流的延迟。
- 短报文和长报文获得公平的调度：如果不同队列间同时存在多个长报文和短报文等待发送，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（协议类型、源和目的 TCP 或 UDP 端口号、源和目的 IP 地址、ToS 域中的优先级位等）自动进行流分类，并且尽可能多地提供队列，以将每个流均匀地放入不同队列中，从而在总体上均衡各个流的延迟。在出队的时候，WFQ 按流的优先级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。

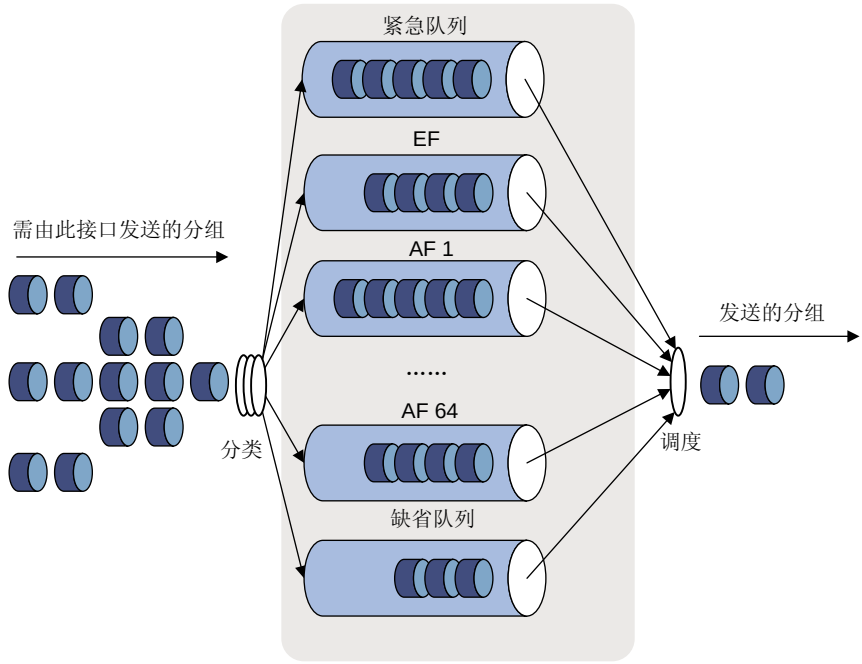
例如：接口中当前共有 5 个流，它们的优先级分别为 0、1、2、3、4，则带宽总配额为所有（流的优先级＋1）的和，即 1＋2＋3＋4＋5＝15。

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 RSVP 协议的保证型业务中，通常就是采用 WFQ 作为调度策略；在流量整形中，也采用 WFQ 调度缓存的报文。

3. CBQ队列

图5-4 基于类的队列示意图



CBQ 是对 WFQ 功能的扩展，为用户提供了定义类的支持。在网络拥塞时，CBQ 根据用户定义的类规则对报文进行匹配，并使其进入相应的队列，在入队列之前必须进行拥塞避免机制和带宽限制的检查。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 包括以下队列：

- 紧急队列：CBQ 提供一个紧急队列，紧急报文入该队列，该队列采用 FIFO 调度，没有带宽限制。
- LLQ：即 EF 队列。如果 CBQ 加权公平对待所有类的队列，实时业务报文（包括语音与视频业务，对延迟比较敏感）就可能得不到及时发送。为此引入一个 EF 队列，为实时业务报文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。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。最多支持 64 个 EF 队列。

- BQ：即 AF 队列。为 AF 业务提供严格、精确的带宽保证，并且保证各类 AF 业务之间按一定的比例关系进行队列调度。最多支持 64 个 AF 队列。
- 缺省队列：一个 WFQ 队列，用来支撑 BE 业务，使用接口剩余带宽进行发送。

系统在为报文匹配规则时，规则如下：

- 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。

5.1.3 拥塞管理技术的对比

设备上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。为了用户更好地利用拥塞管理技术，现对各种队列技术做一比较。

表5-1 拥塞管理技术对比

类型	队列数	优点	缺点
FIFO	1	• 不需要配置，易于使用 • 处理简单，延迟小	• 所有的报文均进入一个“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 • 对不匹配的数据源（即没有流控机制的流，如 UDP 报文发送）无约束力，不匹配的数据源会造成匹配的数据源（如 TCP 报文发送）带宽受损失 • 对时间敏感的实时应用（如 VoIP）的延迟得不到保证
WFQ	可配置	• 配置容易 • 可以保护配合（交互）的数据源（如 TCP 报文发送）的带宽 • 可以减小抖动 • 可以减小数据量小的交互式应用的延迟 • 可以为不同优先级的流分配不同的带宽 • 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

类型	队列数	优点	缺点
CBQ	可配置	• 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 • 可以为 AF 业务提供严格、精确的带宽保证，并且保证各类 AF 业务之间根据权值按一定的比例关系进行队列调度 • 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满足要求；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得不到服务的弊病 • 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

5.2 配置先进先出队列的长度

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。

5.2.1 配置先进先出队列的长度

提示

若是子接口，则接口需要使能 LR 功能以保证队列功能生效。

表5-2 配置先进先出队列的长度

操作		命令	说明
进入系统视图		**system-view**	-
进入接口视图或PVC视图	进入接口视图	**interface** *interface-type interface-number*	二者选其一
	进入PVC视图	**interface atm** *interface-number*	
		pvc *vpi/vci*	
配置先进先出队列的长度		**qos fifo queue-length** *queue-length*	缺省情况下，FIFO队列的长度为75 如果流量突发较大，可以通过增加队列长度的方法来改善队列调度的准确率

5.2.2 FIFO 队列的显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示 FIFO 队列的运行情况，通过查看显示信息验证配置的效果。

表5-3 FIFO 队列的显示和维护

操作	命令
显示接口或PVC先进先出队列配置信息和运行情况	**display qos queue fifo interface** [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]]

5.3 配置加权公平队列

5.3.1 加权公平队列配置过程

提示

若是 Tunnel 接口、子接口、HDLC 捆绑接口或是封装了 PPPoE、PPPoA、PPPoEoA、PPPoFR、MPoFR（FR 接口未使能帧中继流量整形功能）协议的 VT、Dialer 接口，则接口需要使能 LR 功能以保证队列功能生效。

当接口或 PVC 没有使用 WFQ 策略时，使用 **qos wfq** 命令可以使接口或 PVC 使用 WFQ 策略，同时指定 WFQ 的参数。如果接口或 PVC 已经使用了 WFQ 策略，使用 **qos wfq** 命令可以修改 WFQ 的参数。

表5-4 加权公平队列配置过程

操作		命令	说明
进入系统视图		**system-view**	-
进入接口视图或PVC视图	进入接口视图	**interface** *interface-type interface-number*	二者选其一
	进入PVC视图	**interface atm** *interface-number*	
		pvc *vpi/vci*	
配置加权队列		**qos wfq** [**dscp** | **precedence**] [**queue-length** *max-queue-length* | **queue-number** *total-queue-number*] *	缺省情况下，接口或PVC上没有配置WFQ队列

5.3.2 WFQ 队列的显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示 WFQ 队列的运行情况，通过查看显示信息验证配置的效果。

表5-5 WFQ 队列的显示和维护

操作	命令
显示接口或PVC加权公平队列的配置统计信息	**display qos queue wfq interface** [*interface-type interface-number*[**pvc** { *pvc-name* | *vpi/vci* }]]

5.4 配置基于类的队列

5.4.1 配置概述

基于类的队列 CBQ 的配置步骤如下：

(1) 定义类

(2) 定义流行为

(3) 定义策略

(4) 在接口视图下应用 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。

2. 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

3. 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：

- 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%
- 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%
- be：不定义任何特性
- be-flow-based：定义了一个特性为入 WFQ 队列，其中 WFQ 默认有 256 条队列

4. 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：

- 预定义类 ef，采用预定义流行为 ef
- 预定义类 af1～af4，采用预定义流行为 af
- default-class 类，采用预定义流行为 be

5.4.2 定义类

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。

表5-6 定义类

操作	命令	说明
进入系统视图	**system-view**	-
定义一个类，并进入类视图	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	缺省情况下，没有定义类
定义匹配数据包的规则	**if-match** [**not**] *match-criteria*	缺省情况下，没有定义匹配数据包的规则 具体规则请参见QoS命令参考中的命令**if-match**的介绍

5.4.3 定义流行为

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. 配置确保转发（AF），并配置最小可保证带宽

提示

- 该行为只能应用在接口的出方向。
- 在同一流行为视图下 **queue af** 不能与 **queue ef** 命令同时使用。
- 在同一策略下各个类需用同一单位配置 **queue af**，或者用 *bandwidth*，或者用百分比，或者用剩余百分比进行配置。
- 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。当 AF 使用剩余百分比配置的时候，EF 可以使用绝对值或百分比进行配置。

表5-7 配置确保转发（AF），并配置最小可保证带宽

操作	命令	说明
进入系统视图	**system-view**	-
定义一个流行为，并进入流行为视图	**traffic behavior** *behavior-name*	缺省情况下，没有定义流行为
配置确保转发（AF），并配置最小可保证带宽	**queue af bandwidth** { *bandwidth* | **pct** *percentage* | **remaining-pct** *remaining-percentage* }	缺省情况下，没有配置类进行确保转发

2. 配置加速转发（EF），并配置最大带宽

提示

- 在同一流行为视图下 **queue ef** 不能与 **queue af** 和 **queue-length** 命令同时使用。
- 缺省类不能与包含加速转发的行为关联。
- 在同一策略下各个类需用同一单位配置 **queue ef**，或者用 *bandwidth*，或者用百分比进行配置。
- 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。当 AF 使用剩余百分比配置的时候，EF 可以使用绝对值或百分比进行配置。

表5-8 配置加速转发（EF），并配置最大带宽

操作	命令	说明
进入系统视图	**system-view**	-
定义一个流行为，并进入流行为视图	**traffic behavior** *behavior-name*	缺省情况下，没有定义流行为
配置加速转发（EF），并配置最大带宽	**queue ef bandwidth** { *bandwidth* [**cbs** *burst*] | **pct** *percentage* [**cbs-ratio** *ratio*] }	缺省情况下，没有配置类进行加速转发

3. 配置采用公平队列

提示

配置了公平队列的流行为仅可以与缺省类关联使用。

表5-9 配置采用公平队列

操作	命令	说明
进入系统视图	**system-view**	-
定义一个流行为，并进入流行为视图	**traffic behavior** *behavior-name*	缺省情况下，没有定义流行为
配置采用公平队列	**queue wfq** [**queue-number** *total-queue-number*]	缺省情况下，没有为缺省类配置采用公平队列

4. 配置最大队列长度

提示

最大队列长度命令必须在配置了 **queue af** 或 **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。

配置最大队列长度，丢弃方式为尾丢弃。

表5-10 配置最大队列长度

操作	命令	说明
进入系统视图	**system-view**	-
定义一个流行为，并进入流行为视图	**traffic behavior** *behavior-name*	缺省情况下，没有定义流行为
配置最大队列长度	**queue-length** *queue-length*	缺省情况下，丢弃方式为尾部丢弃方式，队列长度为64 如果流量突发较大，可以通过增加队列长度的方法来改善队列调度的准确率

5. 配置丢弃方式为随机丢弃方式

提示

- 在同一流行为视图下 **wred** 不能与 **queue-length** 命令同时使用。
- 必须在配置了 **queue af** 或 **queue wfq** 后使用。
- 删除 WRED 时将删除在该随机丢弃下的其他配置。

表5-11 配置丢弃方式为随机丢弃方式

操作	命令	说明
进入系统视图	**system-view**	-
定义一个流行为，并进入流行为视图	**traffic behavior** *behavior-name*	缺省情况下，没有定义流行为
配置丢弃方式为随机丢弃方式	**wred** [**dscp** | **ip-precedence**]	缺省情况下，没有配置WRED动作

6. 配置WRED计算平均队列长度的指数

提示

必须在配置了 **queue af** 或 **queue wfq**，并已用 **wred** 使能了 WRED 丢弃方式后才可以进行配置。

表5-12 配置 WRED 计算平均队列长度的指数

操作	命令	说明
进入系统视图	**system-view**	-
定义一个流行为并进入流行为视图	**traffic behavior** *behavior-name*	缺省情况下，没有定义流行为
配置WRED计算平均队列长度的指数	**wred weighting-constant** *exponent*	缺省情况下，WRED计算平均队列长度的指数为9

7. 配置WRED各DSCP的下限、上限和丢弃概率分母

提示

- 进行本配置前需已用 **wred dscp** 使能了基于 DSCP 的 WRED 丢弃方式。
- 取消 WRED 配置，**wred dscp** 配置同时被取消。
- 取消 **queue af** 或 **queue wfq** 配置，丢弃参数的配置同时被取消。

表5-13 配置 WRED 各 DSCP 的下限、上限和丢弃概率分母

操作	命令	说明
进入系统视图	**system-view**	-
定义一个流行为并进入流行为视图	**traffic behavior** *behavior-name*	缺省情况下，没有定义流行为
配置WRED各DSCP的下限、上限和丢弃概率分母	**wred dscp** *dscp-value* **low-limit** *low-limit* **high-limit** *high-limit* [**discard-probability** *discard-prob*]	缺省情况下，下限缺省值为10，上限缺省值为30，丢弃概率缺省值为10

8. 配置WRED各IP优先级的下限、上限和丢弃概率分母

提示

- 进行本配置前需已用 **wred ip-precedence** 使能了基于 IP 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** 或 **queue wfq** 配置，丢弃参数的配置同时被取消。

表5-14 配置 WRED 各 IP 优先级的下限、上限和丢弃概率分母

操作	命令	说明
进入系统视图	**system-view**	-
定义一个流行为并进入流行为视图	**traffic behavior** *behavior-name*	缺省情况下，没有定义流行为

操作	命令	说明
配置WRED各优先级的下限、上限和丢弃概率分母	**wred ip-precedence** *precedence* **low-limit** *low-limit* **high-limit** *high-limit* [**discard-probability** *discard-prob*]	缺省情况下，下限缺省值为10，上限缺省值为30，丢弃概率缺省值为10

5.4.4 定义策略

表5-15 在策略中为类指定流行为

操作	命令	说明
进入系统视图	**system-view**	-
定义策略，并进入策略视图	**qos policy** *policy-name*	缺省情况下，没有定义策略
在策略中为类指定采用的流行为	**classifier** *classifier-name* **behavior** *behavior-name*	缺省情况下，没有为类指定流行为

5.4.5 应用策略

qos apply policy 命令将一个策略映射到具体的物理接口或 ATM PVC。一个策略映射可以在多个物理端口或 ATM PVC 上得到应用。

表5-16 将接口或 ATM PVC 与所设置的策略相关联

操作		命令	说明
进入系统视图		**system-view**	-
进入接口视图或PVC视图	进入接口视图	**interface** *interface-type interface-number*	二者选其一 进入接口视图后，下面进行的配置只在当前接口生效；进入PVC视图后，下面进行的配置只在当前PVC生效
	进入PVC视图	**interface atm** *nterface-number*	
		pvc *vpi/vci*	
在接口或PVC上应用关联的策略		**qos apply policy** *policy-name* { **inbound** | **outbound** }	缺省情况下，没有在接口或PVC上应用QoS策略

策略在接口或 ATM PVC 视图下应用的规格如下：

- 普通物理接口，可以应用配置了各种特性（包括 remark、car、queue af、queue ef、queue wfq 等）的策略。
- 配置了队列（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。
- 若是子接口，则接口需要使能 LR 功能以保证 CBQ 队列功能生效。

5.4.6 配置接口最大可用带宽

提示

- 建议最大可用带宽的取值小于物理接口或逻辑链路的实际可用带宽。
- 对于子接口，需要配置该命令以提供 CBQ 计算的基准带宽。

最大可用带宽指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。

表5-17 配置接口最大可用带宽

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置接口最大可用带宽	**bandwidth** *bandwidth-value*	具体情况请参见接口分册命令参考中的介绍

在未配置各种接口的最大可用带宽的条件下，计算 CBQ 时实际使用的基准带宽如下：

- 对于物理接口，其取值为物理接口实际的速率；
- 对于其他虚接口（如 HDLC 捆绑接口），取值为 0kbps。

5.4.7 配置最大预留带宽占可用带宽的百分比

为队列分配带宽时，考虑到部分带宽用于控制协议报文、二层帧头等，通常配置的最大预留带宽不大于可用带宽的 80%。

建议慎重使用该命令修改最大预留带宽。如果配置的最大预留带宽过大，发送的报文加上链路层的帧头有可能大于接口最大可用带宽，导致接口无法满足需求，建议使用缺省最大预留带宽。

表5-18 配置最大预留带宽占可用带宽的百分比

操作		命令	说明
进入系统视图		**system-view**	-
进入接口视图或PVC	进入接口视图	**interface** *interface-type interface-number*	二者选其一
	进入PVC视图	**interface atm** *interface-number*	
		pvc *vpi/vci*	
配置最大预留带宽占可用带宽的百分比		**qos reserved-bandwidth pct** *percent*	最大预留带宽占可用带宽的百分比为80

5.4.8 基于类的队列的显示和维护

在完成上述配置后，在任意视图下执行 **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5-19 基于类的队列的显示和维护

操作	命令
显示设备配置的类信息	**display traffic classifier** { **system-defined** | **user-defined** } [*classifier-name*]
显示设备配置的流行为信息	**display traffic behavior** { **system-defined** | **user-defined** } [*behavior-name*]
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** } [*policy-name* [**classifier** *classifier-name*]]
显示指定接口、指定PVC或所有接口与PVC上上策略的配置信息和运行情况（MSR 2600/MSR 3600）	**display qos policy interface** [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]] [**inbound** | **outbound**]
显示指定接口、指定PVC或所有接口与PVC上上策略的配置信息和运行情况（MSR 5600）	**display qos policy interface** [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]] [**slot** *slot-number*] [**inbound** | **outbound**]
显示指定接口、指定PVC或所有接口与PVC上的基于类的队列配置信息和运行情况	**display qos queue cbq interface** [*interface-type interface-number*[**pvc** { *pvc-name* | *vpi/vci* }]]

5.4.9 基于类的队列典型配置举例

1. 组网需求

在下面的组网图中，从 Router C 发出的数据流经过 Router A 和 Router B 到达 Router D，需求如下：

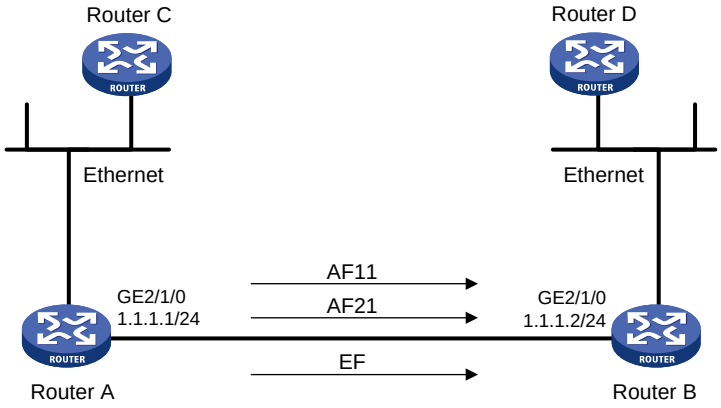
- Router C 发出的数据流根据 IP 报文的 DSCP 域分为 3 类，要求配置 QoS 策略，对于 DSCP 域为 AF11 和 AF21 的流进行确保转发（AF），最小带宽为 5%；
- 对于 DSCP 域为 EF 的流进行加速转发（EF），最大带宽为 30%。

在进行配置之前，应保证：

- Router C 发出的流能够通过 Router A 和 Router B 可达 Router D。
- 报文的 DSCP 域在进入 Router A 之前已经设置完毕。

2. 组网图

图5-5 基于类的队列配置组网图



3. 配置步骤

Router A 上的配置如下。

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

```
<RouterA> system-view
[RouterA] traffic classifier af11_class
[RouterA-classifier-af11_class] if-match dscp af11
[RouterA-classifier-af11_class] quit
[RouterA]traffic classifier af21_class
[RouterA-classifier-af21_class] if-match dscp af21
[RouterA-classifier-af21_class] quit
[RouterA] traffic classifier ef_class
[RouterA-classifier-ef_class] if-match dscp ef
[RouterA-classifier-ef_class] quit
```

定义流行为，配置 AF，并分配最小可用带宽。

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

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

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

定义 QoS 策略，将已配置的流行为指定给不同的类。

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

将已定义的 QoS 策略应用在 Router A 的 GigabitEthernet2/1/0 出方向。

```
[RouterA] interface gigabitethernet 2/1/0
[RouterA-GigabitEthernet2/1/0] ip address 1.1.1.1 255.255.255.0
[RouterA-GigabitEthernet2/1/0] qos apply policy dscp outbound
```

配置完成后，当发生拥塞时，可以观察到 EF 流以较高的优先级转发。

5.5 配置报文信息预提取功能

5.5.1 报文信息预提取功能配置过程

对于 Tunnel 接口对应的物理接口，如果到达对应物理接口的 IP 数据报文已经进行了处理，比如，Tunnel 接口进行了 GRE 封装，此时 QoS 处理的是 GRE 封装后的 IP 数据报文，QoS 无法识别出原始报文的 IP 数据，无法基于原始报文信息对报文进行分类。

使能报文信息预提取功能后，系统在逻辑接口获取原始报文的 IP 数据，并在物理接口应用此 IP 数据，可以基于原始报文信息进行分类，从而进行各种 QoS 处理。

表5-20 报文信息预提取功能配置过程

操作	命令	说明
进入系统视图	**system-view**	-
进入Tunnel接口视图	**interface tunnel** *interface-number*	-
使能报文信息预提取功能	**qos pre-classify**	必选 缺省情况下，Tunnel接口的报文信息预提取功能处于关闭状态

5.5.2 报文信息预提取功能配置举例

1. 组网需求

在 Tunnel 接口上配置报文信息预提取功能。

2. 配置步骤

在接口 Tunnel 0 上使能报文信息预提取功能。

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] qos pre-classify
```

6 拥塞避免

6.1 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。拥塞避免是一种流量控制机制，它通过监视网络资源（如队列或内存缓冲区）的使用情况，在拥塞产生或有加剧的趋势时主动丢弃报文，通过调整网络的流量来避免网络过载。

设备在丢弃报文时，需要与源端的流量控制动作（比如 TCP 流量控制）相配合，调整网络的流量到一个合理的负载状态。丢包策略和源端的流量控制相结合，可以使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。

6.1.1 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，网络不停震荡。

6.1.2 RED 与 WRED

为避免 TCP 全局同步现象，可使用 RED 或 WRED。

RED 和 WRED 通过随机丢弃报文避免了 TCP 的全局同步现象，使得当某个 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。

在 RED 类算法中，为每个队列都设定上限和下限，对队列中的报文进行如下处理：

- 当队列的长度小于下限时，不丢弃报文；
- 当队列的长度超过上限时，丢弃所有到来的报文；
- 当队列的长度在上限和下限之间时，开始随机丢弃到来的报文。队列越长，丢弃概率越高，但有一个最大丢弃概率。

直接采用队列的长度和上限、下限比较并进行丢弃，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。WRED 采用平均队列和设置的队列上限、下限比较来确定丢弃的概率。

队列平均长度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。

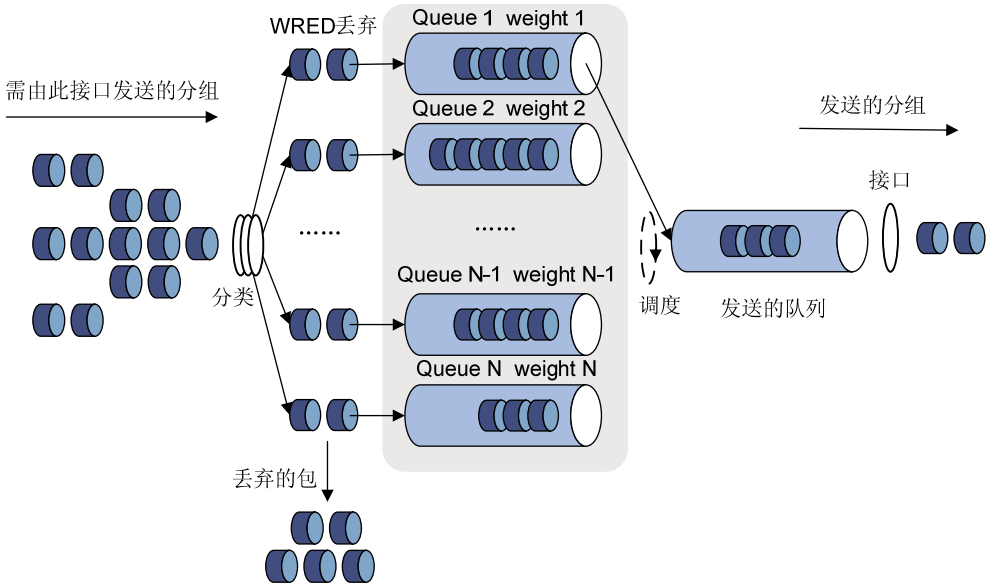
当队列机制采用 WFQ 时，可以为不同优先级的报文设定计算队列平均长度时的指数、上限、下限、丢弃概率，从而对不同优先级的报文提供不同的丢弃特性。

当队列机制采用 FIFO 时，可以为每个队列设定计算队列平均长度时的指数、上限、下限、丢弃概率，为不同类别的报文提供不同的丢弃特性。

6.1.3 WRED 和队列机制的关系

WRED 和队列机制的关系如下图所示。

图6-1 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。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。

6.2 WRED配置说明

6.2.1 WRED 的配置方式

WRED 有两种配置方式：

- 接口配置方式：在接口配置 WRED 的各种参数，并使能 WRED。
- WRED 表配置方式：在系统视图下配置 WRED 表，然后在接口上应用 WRED 表。

目前 MSR 系列路由器仅支持以接口配置方式配置 WRED。

6.2.2 WRED 的参数说明

在进行 WRED 配置时，需要事先确定如下参数：

- 队列上限和下限：当队列平均长度小于下限时，不丢弃报文。当队列平均长度在上限和下限之间时，设备随机丢弃报文，队列越长，丢弃概率越高。当队列平均长度超过上限时，丢弃所有到来的报文。
- 丢弃优先级：在进行报文丢弃时参考的参数，0 对应绿色报文、1 对应黄色报文、2 对应红色报文，红色报文将被优先丢弃。

- 计算平均队列长度的指数：指数越大，计算平均队列长度时对队列的实时变化越不敏感。计算队列平均长度的公式为：平均队列长度=（以前的平均队列长度×（1-1/2^n））＋（当前队列长度×（1/2^n））。其中 n 表示指数。
- 计算丢弃概率的分母：在计算丢弃概率的公式中作为分母。取值越大，计算出的丢弃概率越小。

6.3 以接口配置方式配置WRED

6.3.1 配置过程

表6-1 以接口配置方式配置 WRED 配置过程

操作		命令	说明
进入系统视图		**system-view**	-
进入接口视图或PVC视图	进入接口视图	**interface** *interface-type interface-number*	二者选其一
	进入PVC视图	**interface atm** *interface-number*	
		pvc *vpi/vci*	
使能WRED		**qos wred** [**dscp** | **ip-precedence**] **enable**	缺省情况下，队列丢弃方法为尾丢弃
（可选）配置计算平均队列长度的指数		**qos wred weighting-constant** *exponent*	缺省情况下，WRED计算平均队列长度的指数为9
（可选）配置各优先级对应的参数		**qos wred** { **ip-precedence** *ip-precedence* | **dscp** *dscp-value* } **low-limit** *low-limit* **high-limit** *high-limit* **discard-probability** *discard-prob*	缺省情况下，下限缺省值为10，上限缺省值为30，丢弃概率缺省值为10

6.3.2 配置举例

1. 组网需求

- 在接口 GigabitEthernet2/1/0 上配置基于 IP 优先级的 WRED。
- 配置 IP 优先级为 3 的报文的队列下限为 20、上限为 40、丢弃概率分母为 15。
- 配置计算平均队列长度的指数为 6。

2. 配置步骤

进入系统视图。

```
<Sysname> system-view
```

进入接口视图。

```
[Sysname] interface gigabitethernet 2/1/0
```

使能基于 IP 优先级的 WRED。

```
[Sysname-GigabitEthernet2/1/0] qos wred ip-precedence enable
```

配置优先级为 3 的报文的队列下限为 20，上限为 40，丢弃概率分母为 15。

```
[Sysname-GigabitEthernet2/1/0] qos wred ip-precedence 3 low-limit 20 high-limit 40
discard-probability 15
```

配置计算平均队列长度的指数为 6。

```
[Sysname-GigabitEthernet2/1/0] qos wred weighting-constant 6
```

6.4 WRED显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 WRED 的运行情况，通过查看显示信息验证配置的效果。

表6-2 WRED 显示和维护

操作	命令
显示接口或PVC的WRED配置情况和统计信息	**display qos wred interface** [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]]

7 流量过滤

7.1 流量过滤简介

流量过滤是指对符合流分类的流进行过滤的动作。

例如，可以根据网络的实际情况禁止从某个源 IP 地址发送的报文通过。

7.2 配置流量过滤

表7-1 配置流量过滤

操作		命令	说明
进入系统视图		**system-view**	-
定义一个类，并进入类视图		**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	缺省情况下，没有定义类
定义匹配数据包的规则		**if-match** [**not**] *match-criteria*	缺省情况下，没有定义匹配数据包的规则 具体规则请参见QoS命令参考中的命令**if-match**的介绍
退回系统视图		**quit**	-
定义一个流行为，并进入流行为视图		**traffic behavior** *behavior-name*	缺省情况下，没有定义流行为
配置流量过滤动作		**filter** { **deny** | **permit** }	缺省情况下，没有配置流量统计动作
退回系统视图		**quit**	-
定义一个策略，并进入策略视图		**qos policy** *policy-name*	缺省情况下，没有定义策略
在策略中为类指定采用的流行为		**classifier** *classifier-name* **behavior** *behavior-name*	缺省情况下，没有为类指定流行为
退回系统视图		**quit**	-
应用QoS策略	基于接口或PVC	**2.2.4 1.** 基于接口或PVC应用QoS策略	二者选其一 缺省情况下，没有应用QoS策略
	基于控制平面	**2.2.4 2.** 基于控制平面应用QoS策略	
（可选）显示流量过滤的相关配置信息		**display qos policy user-defined** [*policy-name*]	**display**命令可以在任意视图下执行

7.3 流量过滤配置举例

7.3.1 流量过滤配置举例

1. 组网需求

Host 通过接口 GigabitEthernet2/1/0 接入设备 Router。

配置流量过滤功能，对接口 GigabitEthernet2/1/0 接收的源端口号不等于 21 的 TCP 报文进行丢弃。

2. 组网图

图7-1 流量过滤配置组网图

3. 配置步骤

定义高级 ACL 3000，匹配源端口号不等于 21 的数据流。

```
<Router> system-view
[Router] acl number 3000
[Router-acl-adv-3000] rule 0 permit tcp source-port neq 21
[Router-acl-adv-3000] quit
```

定义类 classifier_1，匹配高级 ACL 3000。

```
[Router] traffic classifier classifier_1
[Router-classifier-classifier_1] if-match acl 3000
[Router-classifier-classifier_1] quit
```

定义流行为 behavior_1，动作为流量过滤（**deny**），对数据包进行丢弃。

```
[Router] traffic behavior behavior_1
[Router-behavior-behavior_1] filter deny
[Router-behavior-behavior_1] quit
```

定义策略 policy，为类 classifier_1 指定流行为 behavior_1。

```
[Router] qos policy policy
[Router-qospolicy-policy] classifier classifier_1 behavior behavior_1
[Router-qospolicy-policy] quit
```

将策略 policy 应用到端口 GigabitEthernet2/1/0 的入方向上。

```
[Router] interface gigabitethernet 2/1/0
[Router-GigabitEthernet2/1/0] qos apply policy policy inbound
```

8 重标记

8.1 重标记简介

重标记是将报文的优先级或者标志位进行设置，重新定义报文的优先级等。例如，对于 IP 报文来说，可以利用重标记对 IP 报文中的 IP 优先级或 DSCP 值进行重新设置，控制 IP 报文的转发。

重标记动作的配置，可以通过与类关联，将原来报文的优先级或标志位重新进行标记。

重标记可以和优先级映射功能配合使用，具体请参见优先级映射章节。

8.2 配置重标记

表8-1 配置重标记

操作		命令	说明
进入系统视图		**system-view**	-
定义一个类，并进入类视图		**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	缺省情况下，没有定义类
定义匹配数据包的规则		**if-match** [**not**] *match-criteria*	缺省情况下，没有定义匹配数据包的规则 具体规则请参见QoS命令参考中的命令**if-match**的介绍
退回系统视图		**quit**	-
定义一个流行为，并进入流行为视图		**traffic behavior** *behavior-name*	缺省情况下，没有定义流行为
重新标记报文的动作	重新标记报文的802.1p优先级	**remark dot1p** *dot1p-value*	五者选其一 缺省情况下，没有配置重新标记报文的动作
	重新标记报文的DSCP值	**remark dscp** *dscp-value*	
	重新标记报文的IP优先级	**remark ip-precedence** *ip-precedence-value*	
	重新标记报文的本地优先级	**remark local-precedence** *local-precedence-value*	
	重新标记报文的QoS本地ID值	**remark qos-local-id** *local-id-value*	
退回系统视图		**quit**	-
定义一个策略，并进入策略视图		**qos policy** *policy-name*	缺省情况下，没有定义策略
在策略中为类指定采用的流行为		**classifier** *classifier-name* **behavior** *behavior-name*	缺省情况下，没有为类指定流行为

操作		命令	说明
退回系统视图		**quit**	-
应用QoS策略	基于接口或PVC	2.2.4 1. 基于接口或PVC应用QoS策略	二者选其一 缺省情况下，没有应用QoS策略
	基于控制平面	2.2.4 2. 基于控制平面应用QoS策略	
（可选）显示重标记的相关配置信息		**display qos policy user-defined** [*policy-name*]	**display**命令可以在任意视图下执行

8.3 重标记配置举例

8.3.1 重标记配置举例

1. 组网需求

公司企业网通过 Router 实现互连。网络环境描述如下：

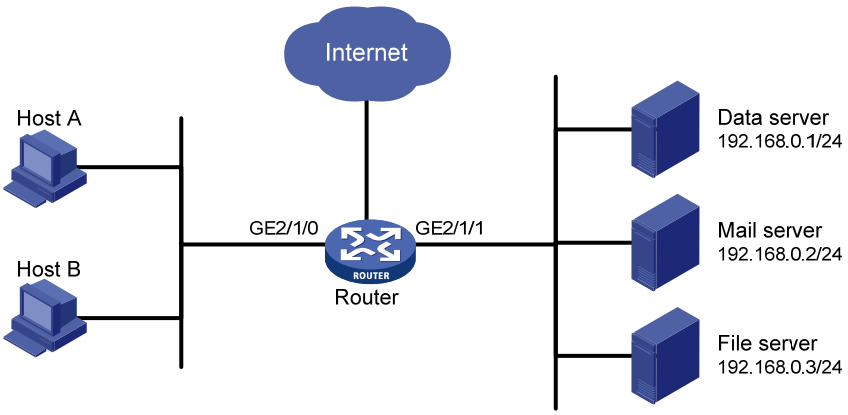
- Host A 和 Host B 通过端口 GigabitEthernet2/1/0 接入 Router；
- 数据库服务器、邮件服务器和文件服务器通过端口 GigabitEthernet2/1/1 接入 Router。

通过配置重标记功能，Router 上实现如下需求：

- 优先处理 Host A 和 Host B 访问数据库服务器的报文；
- 其次处理 Host A 和 Host B 访问邮件服务器的报文；
- 最后处理 Host A 和 Host B 访问文件服务器的报文。

2. 组网图

图8-1 重标记配置组网图



3. 配置步骤

定义高级 ACL 3000，对目的 IP 地址为 192.168.0.1 的报文进行分类。

```
<Router> system-view
[Router] acl number 3000
[Router-acl-adv-3000] rule permit ip destination 192.168.0.1 0
[Router-acl-adv-3000] quit
```

定义高级 ACL 3001，对目的 IP 地址为 192.168.0.2 的报文进行分类。

```
[Router] acl number 3001
[Router-acl-adv-3001] rule permit ip destination 192.168.0.2 0
[Router-acl-adv-3001] quit
```

定义高级 ACL 3002，对目的 IP 地址为 192.168.0.3 的报文进行分类。

```
[Router] acl number 3002
[Router-acl-adv-3002] rule permit ip destination 192.168.0.3 0
[Router-acl-adv-3002] quit
```

定义类 classifier_dbserver，匹配高级 ACL 3000。

```
[Router] traffic classifier classifier_dbserver
[Router-classifier-classifier_dbserver] if-match acl 3000
[Router-classifier-classifier_dbserver] quit
```

定义类 classifier_mserver，匹配高级 ACL 3001。

```
[Router] traffic classifier classifier_mserver
[Router-classifier-classifier_mserver] if-match acl 3001
[Router-classifier-classifier_mserver] quit
```

定义类 classifier_fserver，匹配高级 ACL 3002。

```
[Router] traffic classifier classifier_fserver
[Router-classifier-classifier_fserver] if-match acl 3002
[Router-classifier-classifier_fserver] quit
```

定义流行为 behavior_dbserver，动作为重标记报文的本地优先级为 4。

```
[Router] traffic behavior behavior_dbserver
[Router-behavior-behavior_dbserver] remark local-precedence 4
[Router-behavior-behavior_dbserver] quit
```

定义流行为 behavior_mserver，动作为重标记报文的本地优先级为 3。

```
[Router] traffic behavior behavior_mserver
[Router-behavior-behavior_mserver] remark local-precedence 3
[Router-behavior-behavior_mserver] quit
```

定义流行为 behavior_fserver，动作为重标记报文的本地优先级为 2。

```
[Router] traffic behavior behavior_fserver
[Router-behavior-behavior_fserver] remark local-precedence 2
[Router-behavior-behavior_fserver] quit
```

定义策略 policy_server，为类指定流行为。

```
[Router] qos policy policy_server
[Router-qospolicy-policy_server] classifier classifier_dbserver behavior behavior_dbserver
[Router-qospolicy-policy_server] classifier classifier_mserver behavior behavior_mserver
[Router-qospolicy-policy_server] classifier classifier_fserver behavior behavior_fserver
[Router-qospolicy-policy_server] quit
```

将策略 policy_server 应用到端口 GigabitEthernet2/1/0 上。

```
[Router] interface gigabitethernet 2/1/0
[Router-GigabitEthernet2/1/0] qos apply policy policy_server inbound
[Router-GigabitEthernet2/1/0] quit
```

9 流量重定向

MSR 系列路由器各款型对于本节所描述的特性的支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR 2600	流量重定向	不支持
MSR 3600		配置了HMIM-24GSW接口卡时支持
MSR 5600		配置了HMIM-24GSW接口卡时支持

9.1 流量重定向简介

流量重定向就是将符合流分类的流重定向到其他地方进行处理。

目前支持的流量重定向为重定向到接口，即对于收到需要由某个接口处理的报文时，可以通过配置重定向到此接口。

9.2 配置流量重定向

表9-1 配置流量重定向

操作		命令	说明
进入系统视图		**system-view**	-
定义一个类，并进入类视图		**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	缺省情况下，没有定义类
定义匹配数据包的规则		**if-match** [**not**] *match-criteria*	缺省情况下，没有定义匹配数据包的规则 具体规则请参见QoS命令参考中的命令**if-match**的介绍
退回系统视图		**quit**	-
定义一个流行为，并进入流行为视图		**traffic behavior** *behavior-name*	缺省情况下，没有定义流行为
配置流量重定向动作		**redirect interface** *interface-type interface-number*	缺省情况下，没有配置流量重定向动作
退回系统视图		**quit**	-
定义一个策略，并进入策略视图		**qos policy** *policy-name*	缺省情况下，没有定义策略
在策略中为类指定采用的流行为		**classifier** *classifier-name* **behavior** *behavior-name*	缺省情况下，没有为类指定流行为
退回系统视图		**quit**	-
应用QoS策略	基于接口或PVC	2.2.4 1. 基于接口或PVC应用QoS策略	二者选其一

操作		命令	说明
	基于控制平面	2.2.4 2. 基于控制平面应用QoS策略	缺省情况下，没有应用QoS策略
（可选）显示流量重定向的相关配置信息		**display qos policy user-defined** [*policy-name*]	**display**命令可以在任意视图下执行

9.3 流量重定向配置举例

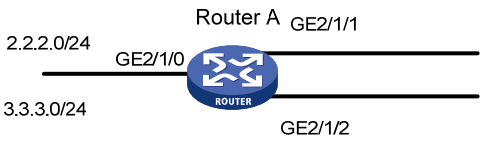
9.3.1 重定向至接口配置举例

1. 组网需求

有两个源网段地址分别为 2.2.2.0/24、3.3.3.0/24 的报文都从 GigabitEthernet2/1/0 接口进入设备，要求做重定向功能，使得这两个网段的报文分别转发至 GigabitEthernet2/1/1 接口和 GigabitEthernet2/1/2 接口。

2. 组网图

图9-1 配置重定向至指定接口



3. 配置步骤

定义基本 ACL 2000，对源网段地址为 2.2.2.0/24 报文进行分类。

```
<RouterA> system-view
[RouterA] acl number 2000
[RouterA-acl-basic-2000] rule permit source 2.2.2.0 0.0.0.255
[RouterA-acl-basic-2000] quit
```

定义基本 ACL 2001，对源网段地址为 3.3.3.0/24 报文进行分类。

```
[RouterA] acl number 2001
[RouterA-acl-basic-2001] rule permit source 3.3.3.0 0.0.0.255
[RouterA-acl-basic-2001] quit
```

定义类 classifier_1，匹配基本 ACL 2000。

```
[RouterA] traffic classifier classifier_1
[RouterA-classifier-classifier_1] if-match acl 2000
[RouterA-classifier-classifier_1] quit
```

定义类 classifier_2，匹配基本 ACL 2001。

```
[RouterA] traffic classifier classifier_2
[RouterA-classifier-classifier_2] if-match acl 2001
[RouterA-classifier-classifier_2] quit
```

定义流行为 behavior_1，动作为重定向至 GigabitEthernet 2/1/1。

```
[RouterA] traffic behavior behavior_1
[RouterA-behavior-behavior_1] redirect interface GigabitEthernet 2/1/1
```

```
[RouterA-behavior-behavior_1] quit
```
定义流行为 behavior_2，动作为重定向至 GigabitEthernet 2/1/2。
```
[RouterA] traffic behavior behavior_2
[RouterA-behavior-behavior_2] redirect interface GigabitEthernet 2/1/2
[RouterA-behavior-behavior_2] quit
```
定义策略 policy，为类 classifier_1 指定流行为 behavior_1，为类 classifier_2 指定流行为 behavior_2。
```
[RouterA] qos policy policy
[RouterA-qospolicy-policy] classifier classifier_1 behavior behavior_1
[RouterA-qospolicy-policy] classifier classifier_2 behavior behavior_2
[RouterA-qospolicy-policy] quit
```
将策略 policy 应用到端口 GigabitEthernet 2/1/0 的入方向上。
```
[RouterA] interface GigabitEthernet 2/1/0
[RouterA-GigabitEthernet 2/1/0] qos apply policy policy inbound
```

10 QPPB

说明

本章所指的路由器代表了一般意义下的路由器，以及运行了路由协议的三层交换机。为提高可读性，在手册的描述中将不另行说明。

10.1 QPPB简介

10.1.1 QPPB 概述

在部署大型复杂网络时，需要执行大量的复杂流分类，而且无法按照团体属性、ACL、Prefix 或 AS-Path 对报文进行分类。如果网络结构不稳定，需经常变化网络结构时，配置修改的工作量非常大甚至难以实施，可以通过部署 QPPB 减少配置修改的工作量。

应用 QPPB 技术可以由 BGP 路由发送者通过设置 BGP 属性预先对路由进行分类。这样在网络拓扑结构发生变化时只需要修改路由发送者上的路由策略就可以满足需求。

QPPB 技术是一项通过 BGP 路由策略部署 QoS 的技术，通过基于 BGP 路由的团体列表、AS-Paths list 和 ACL、Prefix list 等属性进行路由分类，对不同的分类应用不同的 QoS 策略。

QPPB 技术适用于基于目的地址或源地址进行流分类的应用场合，适用于 IBGP 和 EBGP，可以在同一个自治系统内部或者不同的自治系统之间实现。

10.1.2 QPPB 原理

QPPB 技术主要通过 BGP 传播的路由属性设置 QoS 参数，应用 QoS 策略，从而实现 QoS 保障，分为对路由发送者的设置和对路由接收者的设置。

BGP 路由发送者在向邻居发送路由时，先匹配路由策略，为发送的不同路由信息设置不同的 BGP 路由属性。

BGP 邻居在接收到路由后，匹配路由策略，QPPB 可以根据报文的源 IP 地址或目的 IP 地址为接收到的 BGP 路由设置 IP 优先级和 QoS 本地 ID。配置 QoS 策略，根据 IP 优先级和 QoS 本地 ID 对报文进行分类，应用不同的 QoS 策略，从而实现 QoS 保证。

10.2 QPPB配置任务简介

QPPB 的配置可以分为对路由发送者和对路由接收者的配置。

表10-1 QPPB 配置任务简介（8048/CR16K）

配置任务		说明	详细配置
配置发送端	配置发送端的BGP路由	必选	10.2.2 (1)
	配置发送端的路由策略	可选	10.2.2 (2)

配置任务		说明	详细配置
配置接收端	配置接收端的BGP路由	必选	10.2.3 (1)
	配置接收端的路由策略	必选	10.2.3 (2)
	使能QPPB	必选	10.2.3 (3)
	配置QoS策略	必选	10.2.3 (4)
	基于接口应用QoS策略	必选	10.2.3 (5)

10.2.2 配置发送端

路由发送端作为 BGP 路由的发送方，需要根据路由策略设置路由的属性。

(1) 配置 BGP 基本功能

具体配置请参见“三层技术-IP 路由配置指导”中的“BGP”。

(2) 创建路由策略，根据路由策略对不同的路由信息进行分类，并设置不同路由属性

具体配置请参见“三层技术-IP 路由配置指导”中的“路由策略”。

10.2.3 配置接收端

路由接收端作为 BGP 路由的接收方，匹配发送方设置的路由属性，设置 QPPB 相关属性。

(1) 配置 BGP 基本功能

具体配置请参见“三层技术-IP 路由配置指导”中的“BGP”。

(2) 配置路由策略，匹配发送方设置的路由属性，设置 IP 优先级或 QoS 本地 ID

具体配置请参见“三层技术-IP 路由配置指导”中的“路由策略”。

(3) 在接口上配置 QPPB 功能

(4) 配置 QoS 策略

QoS 策略的流分类包含路由策略设置的 IP 优先级和 QoS 本地 ID。

(5) 基于接口应用 QoS 策略

2. 配置QPPB功能

表10-2 配置 QPPB 功能

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置QPPB功能	**bgp-policy** { **destination** | **source** } { **ip-prec-map** | **ip-qos-map** } *	缺省情况下，没有配置QPPB功能 本命令只在流量的入方向生效

3. 基于接口应用QOS策略

表10-3 基于接口应用 QOS 策略

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
应用QoS策略到指定的接口	**qos apply policy** *policy-name* { **inbound** | **outbound** }	缺省情况下，没有在接口上应用QoS策略

10.3 QPPB典型配置举例

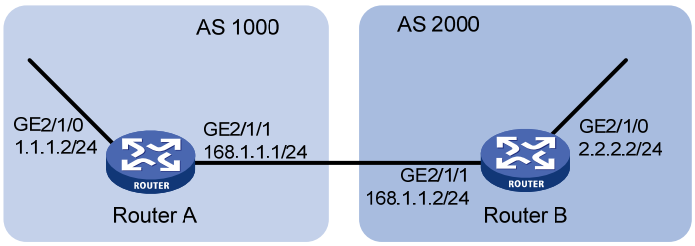
10.3.1 QPPB 在 IPv4 网络中的配置举例

1. 组网需求

如 表 10-4 所示，所有路由器均运行BGP协议。Router B接收路由，根据路由策略对报文进行IP优先级和QoS本地ID的设置，并结合QoS策略进行 512kbps的限速。

2. 组网图

表10-4 QPPB 路由 IPv4 应用配置举例组网图



3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置 Router A

配置 BGP 连接。

```
<RouterA> system-view
[RouterA] bgp 1000
[RouterA-bgp] peer 168.1.1.2 as-number 2000
[RouterA-bgp] peer 168.1.1.2 connect-interface GigabitEthernet 2/1/1
[RouterA-bgp] address-family ipv4
[RouterA-bgp-ipv4] import-route direct
[RouterA-bgp-ipv4] peer 168.1.1.2 enable
[RouterA-bgp-ipv4] quit
[RouterA-bgp] quit
```

(3) 配置 Router B

配置 BGP 连接。

```
<RouterB> system-view
```

```
[RouterB] bgp 2000
[RouterB-bgp] peer 168.1.1.1 as-number 1000
[RouterB-bgp] peer 168.1.1.1 connect-interface gigabitethernet 2/1/1
[RouterB-bgp] address-family ipv4
[RouterB-bgp-ipv4] peer 168.1.1.1 enable
[RouterB-bgp-ipv4] peer 168.1.1.1 route-policy qppb import
[RouterB-bgp-ipv4] quit
[RouterB-bgp] quit
```

配置路由策略。

```
[RouterB] route-policy qppb permit node 0
[RouterB-route-policy-qppb-0] apply ip-precedence 1
[RouterB-route-policy-qppb-0] apply qos-local-id 3
[RouterB-route-policy-qppb-0] quit
```

接口使能 QPPB 能力。

```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] bgp-policy source ip-prec-map ip-qos-map
[RouterB-GigabitEthernet2/1/1] quit
```

配置 QoS 策略。

```
[RouterB] traffic classifier qppb
[RouterB-classifier-qppb] if-match ip-precedence 1
[RouterB-classifier-qppb] if-match qos-local-id 3
[RouterB-classifier-qppb] quit
[RouterB] traffic behavior qppb
[RouterB-behavior-qppb] car cir 512 green pass red discard
[RouterB-behavior-qppb] quit
[RouterB] qos policy qppb
[RouterB-qospolicy-qppb] classifier qppb behavior qppb
[RouterB-qospolicy-qppb] quit
```

接口应用 QoS 策略。

```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] qos apply policy qppb inbound
[RouterB-GigabitEthernet2/1/1] quit
```

4. 验证配置

查看 Router B 相关路由是否生效。

```
[RouterB] display ip routing-table 1.1.1.0 24 verbose

Summary Count : 1

Destination: 1.1.1.0/24
   Protocol: BGP             Process ID: 0
  SubProtID: 0x2                    Age: 00h00m33s
       Cost: 0              Preference: 255
      IpPre: 1              QosLocalID: 3
        Tag: 0                   State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 1000
      NibID: 0x15000000         LastAs: 1000
```

```
     AttrID: 0x0               Neighbor: 168.1.1.1
      Flags: 0x10060        OrigNextHop: 168.1.1.1
      Label: NULL           RealNextHop: 168.1.1.1
    BkLabel: NULL             BkNextHop: N/A
  Tunnel ID: Invalid          Interface: GigabitEthernet2/1/1
BkTunnel ID: Invalid        BkInterface: N/A
```

查看 Router B 的接口 GigabitEthernet2/1/1 上 QoS 策略的配置信息和运行情况。

```
[RouterB] display qos policy interface gigabitethernet 2/1/1

Interface: GigabitEthernet2/1/1

  Direction: Inbound

  Policy: qppb
   Classifier: default-class
     Matched : 51 (Packets) 4022 (Bytes)
     5-minute statistics:
      Forwarded: 0/28 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: be
      -none-
   Classifier: qppb
     Matched : 0 (Packets) 0 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match ip-precedence 1
      If-match qos-local-id 3
     Behavior: qppb
      Committed Access Rate:
        CIR 512 (kbps), CBS 32000 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets) 0 (Bytes)
        Yellow packets: 0 (Packets) 0 (Bytes)
        Red packets   : 0 (Packets) 0 (Bytes)
```

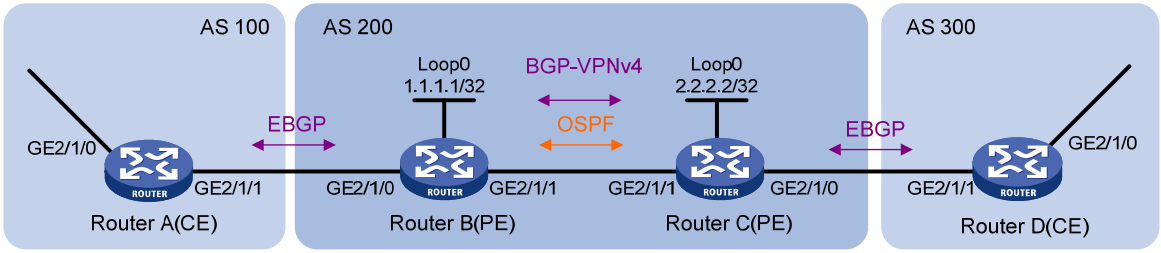
10.3.2 QPPB 在 MPLS L3VPN 中的配置举例

1. 组网需求

如 表 10-5 所示，所有路由器均运行BGP路由协议。Router C接收路由，进行QoS本地ID的设置，并结合QoS策略进行双向 2Mbps的限速。

2. 组网图

表10-5 QPPB 在 MPLS L3VPN 中的配置举例组网图



设备	接口	IP地址	设备	接口	IP地址
Router A	GE2/1/0	192.168.1.2/24	Router B	GE2/1/0	167.1.1.2/24
	GE2/1/1	167.1.1.1/24		GE2/1/1	168.1.1.2/24
Router C	GE2/1/0	169.1.1.2/24	Router D	GE2/1/1	169.1.1.1/24
	GE2/1/1	168.1.1.1/24		GE2/1/0	192.168.3.2/24

3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置 Router A

配置 BGP 连接。

```
<RouterA> system-view
[RouterA] bgp 100
[RouterA-bgp] peer 167.1.1.2 as-number 200
[RouterA-bgp] peer 167.1.1.2 connect-interface gigabitethernet 2/1/1
[RouterA-bgp] address-family ipv4
[RouterA-bgp-ipv4] import-route direct
[RouterA-bgp-ipv4] peer 167.1.1.2 enable
[RouterA-bgp-ipv4] quit
[RouterA-bgp] quit
```

(3) 配置 Router B

配置 VPN 实例。

```
<RouterB> system-view
[RouterB] ip vpn-instance vpn1
[RouterB-vpn-instance-vpn1] route-distinguisher 200:1
[RouterB-vpn-instance-vpn1] vpn-target 200:1 export-extcommunity
[RouterB-vpn-instance-vpn1] vpn-target 200:1 import-extcommunity
[RouterB-vpn-instance-vpn1] quit
```

配置 BGP 连接。

```
[RouterB] router id 1.1.1.1
[RouterB] bgp 200
[RouterB-bgp] peer 2.2.2.2 as-number 200
[RouterB-bgp] peer 2.2.2.2 connect-interface loopback 0
[RouterB-bgp] ip vpn-instance vpn1
[RouterB-bgp-vpn1] peer 167.1.1.1 as-number 100
[RouterB-bgp-vpn1] address-family ipv4
[RouterB-bgp-ipv4-vpn1] peer 167.1.1.1 enable
[RouterB-bgp-ipv4-vpn1] quit
```

```
[RouterB-bgp] address-family vpnv4
[RouterB-bgp-vpnv4] peer 2.2.2.2 enable
[RouterB-bgp-vpnv4] quit
[RouterB-bgp] quit
```

配置 MPLS。

```
[RouterB] mpls lsr-id 1.1.1.1
[RouterB] mpls ldp
[RouterB-mpls-ldp] quit
```

配置 OSPF。

```
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[RouterB-ospf-1-area-0.0.0.0] network 168.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

接口 GigabitEthernet2/1/0 绑定 VPN。

```
[RouterB] interface gigabitethernet 2/1/0
[RouterB-GigabitEthernet2/1/0] ip binding vpn-instance vpn1
[RouterB-GigabitEthernet2/1/0] ip address 167.1.1.2 24
[RouterB-GigabitEthernet2/1/0] quit
```

接口 GigabitEthernet2/1/1 使能 MPLS。

```
[RouterB] interface gigabitethernet 2/1/1
[RouterB-GigabitEthernet2/1/1] mpls enable
[RouterB-GigabitEthernet2/1/1] mpls ldp enable
[RouterB-GigabitEthernet2/1/1] quit
```

(4) 配置 Router C

配置 VPN 实例。

```
<RouterC> system-view
[RouterC] ip vpn-instance vpn1
[RouterC-vpn-instance-vpn1] route-distinguisher 200:1
[RouterC-vpn-instance-vpn1] vpn-target 200:1 export-extcommunity
[RouterC-vpn-instance-vpn1] vpn-target 200:1 import-extcommunity
[RouterC-vpn-instance-vpn1] quit
```

配置 BGP 连接。

```
[RouterC] router id 2.2.2.2
[RouterC] bgp 200
[RouterC-bgp] peer 1.1.1.1 as-number 200
[RouterC-bgp] peer 1.1.1.1 connect-interface loopback 0
[RouterC-bgp] ip vpn-instance vpn1
[RouterC-bgp-vpn1] peer 169.1.1.1 as-number 300
[RouterC-bgp-vpn1] address-family ipv4
[RouterC-bgp-ipv4-vpn1] peer 169.1.1.1 enable
[RouterC-bgp-ipv4-vpn1] peer 169.1.1.1 route-policy qppb import
[RouterC-bgp-ipv4-vpn1] quit
[RouterC-bgp-vpn1] quit
[RouterC-bgp] address-family vpnv4
[RouterC-bgp-vpnv4] peer 1.1.1.1 enable
```

```
[RouterC-bgp-vpnv4] peer 1.1.1.1 route-policy qppb import
[RouterC-bgp-vpnv4] quit
[RouterC-bgp] quit
```
配置路由策略。
```
[RouterC] route-policy qppb permit node 0
[RouterC-route-policy-qppb-0] apply qos-local-id 1023
[RouterC-route-policy-qppb-0] quit
```
配置 MPLS。
```
[RouterC] mpls lsr-id 2.2.2.2
[RouterC] mpls ldp
[RouterC-mpls-ldp] quit
```
配置 OSPF。
```
[RouterC] ospf
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[RouterC-ospf-1-area-0.0.0.0] network 168.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```
配置 QoS 策略。
```
[RouterC] traffic classifier qppb
[RouterC-classifier-qppb] if-match qos-local-id 1023
[RouterC-classifier-qppb] quit
[RouterC] traffic behavior qppb
[RouterC-behavior-qppb] car cir 2000 green pass red discard
[RouterC-behavior-qppb] quit
[RouterC] qos policy qppb
[RouterC-qospolicy-qppb] classifier qppb behavior qppb
[RouterC-qospolicy-qppb] quit
```
接口 GigabitEthernet2/1/1 使能 MPLS。
```
[RouterC] interface gigabitethernet 2/1/1
[RouterC-GigabitEthernet2/1/1] mpls enable
[RouterC-GigabitEthernet2/1/1] mpls ldp enable
```
接口使能 QPPB 能力。
```
[RouterC-GigabitEthernet2/1/1] bgp-policy destination ip-qos-map
[RouterC-GigabitEthernet2/1/1] quit
[RouterC] interface gigabitethernet 2/1/0
[RouterC-GigabitEthernet2/1/0] bgp-policy destination ip-qos-map
[RouterC-GigabitEthernet2/1/0] quit
```
接口 GigabitEthernet2/1/0 绑定 VPN。
```
[RouterC] interface gigabitethernet 2/1/0
[RouterC-GigabitEthernet2/1/0] ip binding vpn-instance vpn1
[RouterC-GigabitEthernet2/1/0] ip address 169.1.1.2 24
```
接口 GigabitEthernet2/1/0 应用 QoS 策略。
```
[RouterC-GigabitEthernet2/1/0] qos apply policy qppb inbound
[RouterC-GigabitEthernet2/1/0] qos apply policy qppb outbound
```
(5)　配置 Router D

配置 BGP 连接。

```
<RouterD> system-view
[RouterD] bgp 300
[RouterD-bgp] peer 169.1.1.2 as-number 200
[RouterD-bgp] peer 169.1.1.2 connect-interface gigabitethernet 2/1/1
[RouterD-bgp] address-family ipv4
[RouterD-bgp-ipv4] peer 169.1.1.2 enable
[RouterD-bgp-ipv4] import-route direct
[RouterD-bgp-ipv4] quit
```

4. 验证配置

查看 Router A 相关路由是否生效。

```
[RouterA] display ip routing-table

Destinations : 18        Routes : 18

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
167.1.1.0/24        Direct 0    0            167.1.1.1       GE2/1/1
167.1.1.0/32        Direct 0    0            167.1.1.1       GE2/1/1
167.1.1.1/32        Direct 0    0            127.0.0.1       InLoop0
167.1.1.255/32      Direct 0    0            167.1.1.1       GE2/1/1
169.1.1.0/24        BGP    255  0            167.1.1.2       GE2/1/1
192.168.1.0/24      Direct 0    0            192.168.1.2     GE2/1/0
192.168.1.0/32      Direct 0    0            192.168.1.2     GE2/1/0
192.168.1.2/32      Direct 0    0            127.0.0.1       InLoop0
192.168.1.255/32    Direct 0    0            192.168.1.2     GE2/1/0
192.168.3.0/24      BGP    255  0            167.1.1.2       GE2/1/1
224.0.0.0/4         Direct 0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0            0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

查看 Router B 相关路由是否生效。

```
[RouterB] display ip routing-table

Destinations : 14        Routes : 14

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
1.1.1.1/32          Direct 0    0            127.0.0.1       InLoop0
2.2.2.2/32          OSPF   10   1            168.1.1.1       GE2/1/1
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

```
168.1.1.0/24        Direct 0    0           168.1.1.2       GE2/1/1
168.1.1.0/32        Direct 0    0           168.1.1.2       GE2/1/1
168.1.1.2/32        Direct 0    0           127.0.0.1       InLoop0
168.1.1.255/32      Direct 0    0           168.1.1.2       GE2/1/1
224.0.0.0/4         Direct 0    0           0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0           0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
[RouterB] display ip routing-table vpn-instance vpn1

Destinations : 16        Routes : 16

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
0.0.0.0/32          Direct 0    0           127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0           127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0           127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
167.1.1.0/24        Direct 0    0           167.1.1.2       GE2/1/0
167.1.1.0/32        Direct 0    0           167.1.1.2       GE2/1/0
167.1.1.2/32        Direct 0    0           127.0.0.1       InLoop0
167.1.1.255/32      Direct 0    0           167.1.1.2       GE2/1/0
169.1.1.0/24        BGP    255  0           2.2.2.2         GE2/1/1
192.168.1.0/24      BGP    255  0           167.1.1.1       GE2/1/0
192.168.2.0/24      BGP    255  0           167.1.1.1       GE2/1/0
192.168.3.0/24      BGP    255  0           2.2.2.2         GE2/1/1
224.0.0.0/4         Direct 0    0           0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0           0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
```

查看 Router C 相关路由是否生效。

```
[RouterC] display ip routing-table

Destinations : 14        Routes : 14

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
0.0.0.0/32          Direct 0    0           127.0.0.1       InLoop0
1.1.1.1/32          OSPF   10   1           168.1.1.2       GE2/1/1
2.2.2.2/32          Direct 0    0           127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0           127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0           127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
168.1.1.0/24        Direct 0    0           168.1.1.1       GE2/1/1
168.1.1.0/32        Direct 0    0           168.1.1.1       GE2/1/1
168.1.1.1/32        Direct 0    0           127.0.0.1       InLoop0
168.1.1.255/32      Direct 0    0           168.1.1.1       GE2/1/1
224.0.0.0/4         Direct 0    0           0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0           0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
```

```
[RouterC] display ip routing-table vpn-instance vpn1

Destinations : 16        Routes : 16

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
167.1.1.0/24        BGP    255  0            1.1.1.1         GE2/1/1
169.1.1.0/24        Direct 0    0            169.1.1.2       GE2/1/0
169.1.1.0/32        Direct 0    0            169.1.1.2       GE2/1/0
169.1.1.2/32        Direct 0    0            127.0.0.1       InLoop0
169.1.1.255/32      Direct 0    0            169.1.1.2       GE2/1/0
192.168.1.0/24      BGP    255  0            1.1.1.1         GE2/1/1
192.168.2.0/24      BGP    255  0            169.1.1.1       GE2/1/0
192.168.3.0/24      BGP    255  0            169.1.1.1       GE2/1/0
224.0.0.0/4         Direct 0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0            0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

查看 Router D 相关路由是否生效。

```
[RouterD] display ip routing-table

Destinations : 18        Routes : 18

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
167.1.1.0/24        BGP    255  0            169.1.1.2       GE2/1/1
169.1.1.0/24        Direct 0    0            169.1.1.1       GE2/1/1
169.1.1.0/32        Direct 0    0            169.1.1.1       GE2/1/1
169.1.1.1/32        Direct 0    0            127.0.0.1       InLoop0
169.1.1.255/32      Direct 0    0            169.1.1.1       GE2/1/1
192.168.1.0/24      BGP    255  0            169.1.1.2       GE2/1/1
192.168.3.0/24      Direct 0    0            192.168.3.2     GE2/1/0
192.168.3.0/32      Direct 0    0            192.168.3.2     GE2/1/0
192.168.3.2/32      Direct 0    0            127.0.0.1       InLoop0
192.168.3.255/32    Direct 0    0            192.168.3.2     GE2/1/0
224.0.0.0/4         Direct 0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0            0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

查看 Router C 的接口 GigabitEthernet2/1/0 上 QoS 策略的配置信息和运行情况。

```
[RouterC] display qos policy interface gigabitethernet 2/1/0
```

```
Interface: GigabitEthernet2/1/0

  Direction: Inbound

  Policy: qppb
   Classifier: default-class
     Matched : 312 (Packets) 18916 (Bytes)
     5-minute statistics:
      Forwarded: 0/24 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: be
      -none-
   Classifier: qppb
     Matched : 0 (Packets) 0 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match qos-local-id 1023
     Behavior: qppb
      Committed Access Rate:
        CIR 2000 (kbps), CBS 125000 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets) 0 (Bytes)
        Yellow packets: 0 (Packets) 0 (Bytes)
        Red packets   : 0 (Packets) 0 (Bytes)

  Direction: Outbound

  Policy: qppb
   Classifier: default-class
     Matched : 311 (Packets) 23243 (Bytes)
     5-minute statistics:
      Forwarded: 0/24 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: be
      -none-
   Classifier: qppb
     Matched : 0 (Packets) 0 (Bytes)
```

```
5-minute statistics:
 Forwarded: 0/0 (pps/bps)
 Dropped  : 0/0 (pps/bps)
Operator: AND
Rule(s) :
 If-match qos-local-id 1023
Behavior: qppb
 Committed Access Rate:
   CIR 2000 (kbps), CBS 125000 (Bytes), EBS 512 (Bytes)
   Green action  : pass
   Yellow action : pass
   Red action    : discard
   Green packets : 0 (Packets) 0 (Bytes)
   Yellow packets: 0 (Packets) 0 (Bytes)
   Red packets   : 0 (Packets) 0 (Bytes)
```

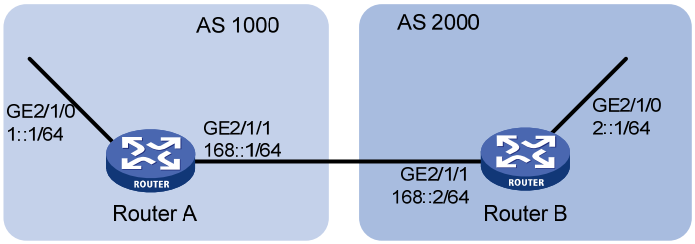
10.3.3 QPPB 在 IPv6 网络中的配置举例

1. 组网需求

如 表 10-6 所示，所有路由器均运行BGP协议。Router B接收路由，进行IP优先级设置，并结合QoS策略进行 512kbps的限速。

2. 组网图

表10-6 QPPB 在 IPv6 网络中的配置举例组网图



3. 配置步骤

(1) 配置各接口的 IPv6 地址（略）

(2) 配置 Router A

配置 BGP

```
<RouterA> system-view
[RouterA] bgp 1000
[RouterA] peer 168::2 as-number 2000
[RouterA] peer 168::2 connect-interface gigabitethernet 2/1/1
[RouterA-bgp] address-family ipv6
[RouterA-bgp-ipv6] peer 168::2 enable
[RouterA-bgp-ipv6] import-route direct
[RouterA-bgp-ipv6] quit
[RouterA-bgp] quit
```

(3) 配置 Router B

配置 BGP

```
<RouterB> system-view
[RouterB] bgp 2000
[RouterB] peer 168::1 as-number 1000
[RouterB] peer 168::1 connect-interface gigabitethernet 2/1/1
[RouterB-bgp] address-family ipv6
[RouterB-bgp-ipv6] peer 168::1 enable
[RouterB-bgp-ipv6] peer 168::1 route-policy qppb import
[RouterB-bgp-ipv6] quit
[RouterB-bgp] quit
```

配置路由策略

```
[RouterB] route-policy qppb permit node 0
[RouterB-route-policy-qppb-0] apply ip-precedence 4
[RouterB-route-policy-qppb-0] quit
```

接口使能 QPPB 能力

```
[RouterB] interface gigabitethernet 2/1/0
[RouterB-GigabitEthernet2/1/0] bgp-policy destination ip-prec-map
```

配置 QoS 策略。

```
[RouterB] traffic classifier qppb
[RouterB-classifier-qppb] if-match ip-precedence 4
[RouterB-classifier-qppb] quit
[RouterB] traffic behavior qppb
[RouterB-behavior-qppb] car cir 512 red discard
[RouterB-behavior-qppb] quit
[RouterB] qos policy qppb
[RouterB-qospolicy-qppb] classifier qppb behavior qppb
[RouterB-qospolicy-qppb] quit
```

接口应用 QoS 策略。

```
[RouterB] interface gigabitethernet 2/1/0
[RouterB-GigabitEthernet2/1/0] qos apply policy qppb inbound
[RouterB-GigabitEthernet2/1/0] quit
```

4. 验证配置

查看 Router A 相关路由是否生效。

```
[RouterA] display ipv6 routing-table

Destinations : 7        Routes : 7

Destination: ::1/128                                    Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 1::/64                                     Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : GE2/1/0                                     Cost      : 0

Destination: 1::1/128                                   Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0
```

```
Destination: 168::/64                                   Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : GE2/1/1                                     Cost      : 0

Destination: 168::1/128                                 Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: FE80::/10                                  Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0

Destination: FF00::/8                                   Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0
```

查看 Router B 相关路由是否生效。

```
[RouterB] display ipv6 routing-table

Destinations : 9 Routes : 9

Destination: ::1/128                                    Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 1::/64                                     Protocol  : BGP4+
NextHop    : 168::1                                     Preference: 255
Interface  : GE2/1/1                                     Cost      : 0

Destination: 2::/64                                     Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : GE2/1/0                                     Cost      : 0

Destination: 2::1/128                                   Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 2::2/128                                   Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 168::/64                                   Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : GE2/1/1                                     Cost      : 0

Destination: 168::2/128                                 Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0
```

```
Destination: FE80::/10                                  Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0

Destination: FF00::/8                                   Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0
```

查看 Router B 的接口 GigabitEthernet2/1/0 上 QoS 策略的配置信息和运行情况。

```
[RouterC] display qos policy interface gigabitethernet 2/1/0

Interface: GigabitEthernet2/1/0

  Direction: Inbound

  Policy: qppb
   Classifier: default-class
     Matched : 0 (Packets) 0 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: be
      -none-
   Classifier: qppb
     Matched : 0 (Packets) 0 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match ip-precedence 4
     Behavior: qppb
      Committed Access Rate:
        CIR 512 (kbps), CBS 32000 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets) 0 (Bytes)
        Yellow packets: 0 (Packets) 0 (Bytes)
        Red packets   : 0 (Packets) 0 (Bytes)
```

11 附录

11.1 附录 A 缩略语表

表11-1 附录 A 缩略语表

缩略语	英文全名	中文解释
AF	Assured Forwarding	确保转发
BE	Best Effort	尽力转发
BQ	Bandwidth Queuing	带宽队列
CAR	Committed Access Rate	承诺访问速率
CBQ	Class Based Queuing	基于类的队列
CBS	Committed Burst Size	承诺突发尺寸
CBWFQ	Class Based Weighted Fair Queuing	基于类的加权公平队列
CE	Customer Edge	用户边缘设备
CIR	Committed Information Rate	承诺信息速率
CQ	Custom Queuing	定制队列
DiffServ	Differentiated Service	区分服务
DoS	Denial of Service	拒绝服务
DSCP	Differentiated Services Code Point	区分服务编码点
EBS	Excess Burst Size	超出突发尺寸
EF	Expedited Forwarding	加速转发
FEC	Forwarding Equivalance Class	转发等价类
FIFO	First in First out	先入先出
FQ	Fair Queuing	公平队列
GTS	Generic Traffic Shaping	通用流量整形
IntServ	Integrated Service	综合服务
ISP	Internet Service Provider	互联网服务提供商
LFI	Link Fragmentation and Interleaving	链路分片与交叉
LLQ	Low Latency Queuing	低时延队列
LR	Line Rate	物理接口限速
LSP	Label Switched Path	标签交换路径
MPLS	Multiprotocol Label Switching	多协议标签交换

缩略语	英文全名	中文解释
PE	Provider Edge	服务提供商网络边缘
PIR	Peak Information Rate	峰值信息速率
PQ	Priority Queuing	优先队列
QoS	Quality of Service	服务质量
QPPB	QoS Policy Propagation Through the Border Gateway Protocol	通过BGP传播QoS策略
RED	Random Early Detection	随机早期检测
RSVP	Resource Reservation Protocol	资源预留协议
RTP	Real-time Transport Protocol	实时传输协议
TE	Traffic Engineering	流量工程
ToS	Type of Service	服务类型
TP	Traffic Policing	流量监管
TS	Traffic Shaping	流量整形
VoIP	Voice over IP	在IP网络上传送语音
VPN	Virtual Private Network	虚拟专用网络
WFQ	Weighted Fair Queuing	加权公平队列
WRED	Weighted Random Early Detection	加权随机早期检测

11.2 附录 B 缺省优先级映射表（不带颜色）

表11-2 dot1p-lp 缺省映射关系

映射输入索引	dot1p-lp 映射
dot1p	lp
0	2
1	0
2	1
3	3
4	4
5	5
6	6

映射输入索引	dot1p-lp 映射
7	7

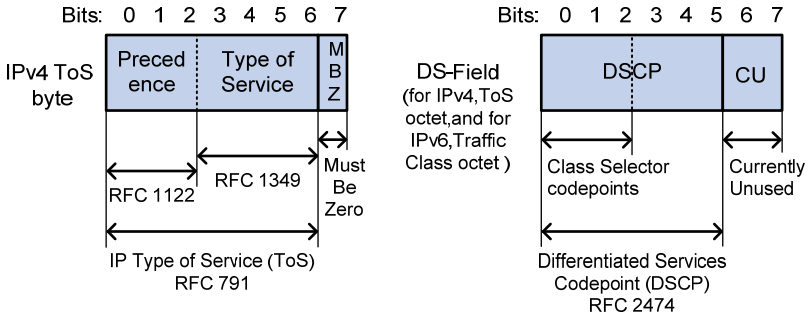
表11-3 dscp-lp 缺省映射关系

映射输入索引	dscp-lp 映射
dscp	lp
0～7	0
8～15	1
16～23	2
24～31	3
32～39	4
40～47	5
48～55	6
56～63	7

11.3 附录 C 各种优先级介绍

11.3.1 IP 优先级和 DSCP 优先级

图11-1 ToS 和 DS 域



如 图 11-1 所示，IP报文头的ToS字段有 8 个bit，其中前 3 个bit表示的就是IP优先级，取值范围为 0～7。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11-4 IP 优先级说明

IP 优先级（十进制）	IP 优先级（二进制）	关键字
0	000	routine
1	001	priority

IP 优先级（十进制）	IP 优先级（二进制）	关键字
2	010	immediate
3	011	flash
4	100	flash-override
5	101	critical
6	110	internet
7	111	network

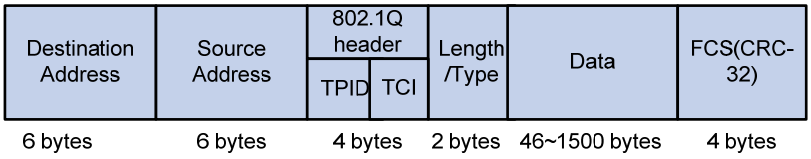
表11-5 DSCP 优先级说明

DSCP 优先级（十进制）	DSCP 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
40	101000	cs5
48	110000	cs6
56	111000	cs7
0	000000	be（default）

11.3.2 802.1p 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11-2 带有 802.1Q 标签头的以太网帧



如 图 11-2 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，图 11-3 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11-3 802.1Q 标签头

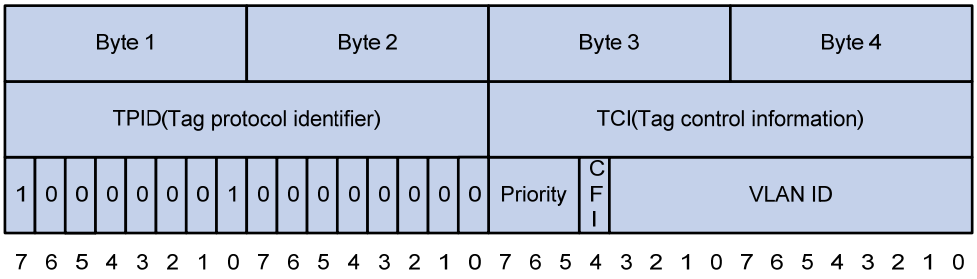


表11-6 802.1p 优先级说明

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
7	111	network-management

目 录

1 MPLS QoS

1.1 MPLS QoS概述

MPLS QoS 是部署 QoS 业务的重要组成部分，在实际的 MPLS 组网方案中往往通过差分服务模型来实施 QoS。MPLS 的相关内容请参见“MPLS 配置指导”中的“MPLS 基础”。

MPLS QoS 与传统 IP QoS 的不同在于，传统的 IP QoS 根据 IP 优先级来判断业务的服务等级，实现差分服务；MPLS QoS 则需要根据 EXP 的值来区分不同的数据流，实现差分服务，保证关键业务（例如，语音和视频）数据流的低延时、低丢包率，保证网络的高利用率。

MPLS QoS 主要完成以下功能：

- 根据需要在 PE 上对业务流进行分类。例如，可以将 EXP 值为 1 的流分为一类，EXP 值为 2 的流分为一类，对分类后的流量可以进行流量监管和重标记。
- PE 在给报文加 Label 时，把 IP 报文携带的 IP 优先级标记映射到标签的 EXP 域，这样原来由 IP 携带的类型信息，现在由标签携带。
- 在 P 和 PE 之间，根据标签的 EXP 域，进行有差别的调度（如 PQ、WFQ、CBQ 等），即在一条 LSP 上为携带标签的业务流提供有差别的 QoS。

说明

MPLS 标签中 EXP 字段的处理采用如下原则：

- 给 IP 报文封装 MPLS 标签时，直接将 IP 报文的 ToS 字段转换成 MPLS 标签的 EXP 字段；标签交换（swap）操作时，EXP 字段保持不变；标签压栈（push）操作时，新压入的外层标签 EXP 字段继承内层标签的 EXP 字段；标签弹栈（pop）操作时，不会将弹出标签的 EXP 字段复制到内层标签或 IP 报文的 ToS 字段上。
- 重标记 EXP 只修改最外层标签的 EXP 字段值。

1.2 MPLS QoS配置

配置 MPLS QoS 之前，请先完成 MPLS 基本功能的配置。MPLS 基本功能的相关配置请参见“MPLS 配置指导”中的“MPLS 基础”。

1.2.1 配置MPLS的流量监管

通过对进入 MPLS 网络的报文进行流量监管，可以限定报文的传送速率，避免网络拥塞的发生，并可以对报文重新标记优先级。流量监管的相关内容请参见“ACL 和 QoS 配置指导”中的“流量监管、流量整形和接口限速”。

表1-1 配置 MPLS 的流量监管

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
进入接口视图	**interface** *interface-type interface-number*	-
在接口上应用MPLS CAR	**qos car** { **inbound** | **outbound** } { **any** | **acl** [**ipv6**] *acl-number* } **cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**pir** *peak-information-rate*] [**green** *action* | **red** *action* | **yellow** *action*] *	缺省情况下，接口上没有配置CAR

action 中关于 MPLS 的动作如下：

- **remark-mpls-exp-continue** *new-exp*：设置新的 MPLS 报文的 EXP 标志位的值，并继续由下一个 CAR 策略处理，取值范围 0～7。
- **remark-mpls-exp-pass** *new-exp*：设置新的 MPLS 报文的 EXP 标志位的值，并允许数据包通过，取值范围 0～7。

1.2.2 配置MPLS的重标记

在 MPLS 网络中，若要通过 EXP 域对 MPLS 报文分类并提供不同的服务，依据匹配的流量类别在 MPLS 中重新标记优先级后转发，需要配置 MPLS 的重标记。重标记的相关内容请参见“ACL 和 QoS 配置指导”中的“重标记”。

表1-2 配置 MPLS 的重标记

操作	命令	说明
进入系统视图	**system-view**	-
定义一个类，并进入类视图	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	缺省情况下，没有定义类
定义匹配数据包的规则	**if-match** [**not**] **mpls-exp** *exp-value*&<1-8>	缺省情况下，没有定义匹配数据包的规则 该规则仅对MPLS报文有效，对IP报文无效
退回系统视图	**quit**	-
定义一个流行为，并进入流行为视图	**traffic behavior** *behavior-name*	缺省情况下，没有定义流行为
标记MPLS报文的EXP值	**remark mpls-exp** *exp-value*	缺省情况下，没有配置重新标记报文的动作
退回系统视图	**quit**	-
定义一个策略，并进入策略视图	**qos policy** *policy-name*	缺省情况下，没有定义策略
将MPLS QoS策略的类和流行为进行绑定	**classifier** *classifier-name* **behavior** *behavior-name*	缺省情况下，没有为类指定流行为
退回系统视图	**quit**	-

操作	命令	说明
基于接口应用QoS策略	相关内容请参见“ACL和QoS配置指导”中的“QoS配置方式”	缺省情况下，没有应用QoS策略

目 录

1 时间段

1.1 时间段简介

时间段（Time Range）定义了一个时间范围。用户通过创建一个时间段并在某业务中将其引用，就可使该业务在此时间段定义的时间范围内生效。但如果一个业务所引用的时间段尚未配置或已被删除，该业务将不会生效。

譬如，当一个 ACL 规则只需在某个特定时间范围内生效时，就可以先配置好这个时间段，然后在配置该 ACL 规则时引用此时间段，这样该 ACL 规则就只能在该时间段定义的时间范围内生效。

时间段可分为以下两种类型：

- 周期时间段：表示以一周为周期（如每周一的 8 至 12 点）循环生效的时间段。
- 绝对时间段：表示在指定时间范围内（如 2013 年 1 月 1 日 8 点至 2013 年 1 月 3 日 18 点）生效时间段。

每个时间段都以一个名称来标识，用户最多可创建 1024 个不同名称的时间段。一个时间段内可包含一或多个周期时间段（最多 32 个）和绝对时间段（最多 12 个），当一个时间段内包含有多个周期时间段和绝对时间段时，系统将先分别取各周期时间段的并集和各绝对时间段的并集，再取这两个并集的交集作为该时间段最终生效的时间范围。

1.2 配置时间段

表1-1 配置时间段

操作	命令	说明
进入系统视图	**system-view**	-
创建时间段	**time-range** *time-range-name* { *start-time* **to** *end-time* *days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* }	缺省情况下，不存在任何时间段

1.3 时间段显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示时间段配置后的运行情况，通过查看显示信息验证配置的效果。

表1-2 时间段显示和维护

配置	命令
显示时间段的配置和状态信息	**display time-range** { *time-range-name* | **all** }

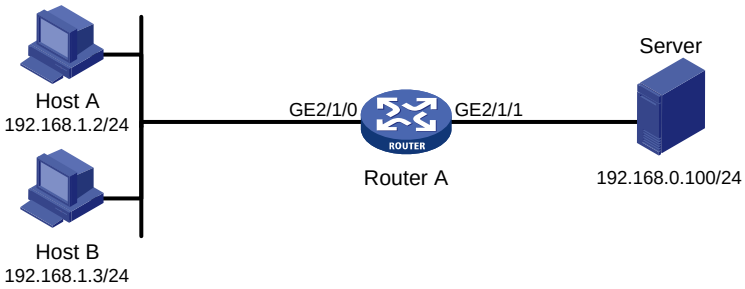
1.4 时间段典型配置举例

1. 组网需求

要求通过在 Router A 上配置 ACL 规则，实现在 2013 年 6 月到 2013 年 12 月之间每周工作日的 8 点到 18 点只允许 Host A 访问 Server。

2. 组网图

图1-1 时间段典型配置组网图



3. 配置步骤

创建名为 work 的时间段，其时间范围为 2013 年 6 月到 2013 年 12 月之间每周工作日的 8 点到 18 点。

```
<RouterA> system-view
[RouterA] time-range work 08:00 to 18:00 working-day from 00:00 6/1/2013 to 24:00 12/31/2013
```

创建 IPv4 基本 ACL 2001，并制订如下规则：在名为 work 的时间段内只允许来自 192.168.1.2/32 的报文通过、禁止来自其它 IP 地址的报文通过。

```
[RouterA] acl number 2001
[RouterA-acl-basic-2001] rule permit source 192.168.1.2 0 time-range work
[RouterA-acl-basic-2001] rule deny source any time-range work
[RouterA-acl-basic-2001] quit
```

应用 IPv4 基本 ACL 2001 对接口 GigabitEthernet2/1/1 出方向上的报文进行过滤。

```
[RouterA] interface gigabitethernet 2/1/1
[RouterA-GigabitEthernet2/1/1] packet-filter 2001 outbound
[RouterA-GigabitEthernet2/1/1] quit
```

4. 验证配置

配置完成后，在 Router A 上可以使用 **display time-range** 命令查看时间段的配置和状态信息：

显示所有时间段的配置和状态信息。

```
[RouterA] display time-range all
Current time is 13:58:35 6/19/2013 Friday

Time-range : work (Active)
 08:00 to 18:00 working-day
 from 00:00 6/1/2013 to 00:00 1/1/2014
```

由此可见，时间段 work 已经生效。