H3C MSR 系列路由器

ACL 和 QoS 命令参考(V5)

新华三技术有限公司
http://www.h3c.com

资料版本：20180820-C-1.14
产品版本：MSR-CMW520-R2511P07

前 言

本命令参考(V5)共分为十七本手册，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 命令参考》主要介绍访问控制列表及 QoS 相关的命令。

前言部分包含如下内容：

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. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下

格　式	意　义
	的[文件夹]菜单项。

3. 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。

4. 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。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。

	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

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。

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配置

1.1 ACL配置命令

1.1.1 acl

【命令】

acl number *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]

undo acl { **all** | **name** *acl-name* | **number** *acl-number* }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

number *acl-number*：指定 ACL 的编号。*acl-number* 表示 ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 100～199：表示 WLAN ACL；
- 2000～2999：表示 IPv4 基本 ACL；
- 3000～3999：表示 IPv4 高级 ACL；
- 4000～4999：表示二层 ACL；
- 5000～5999：表示用户自定义 ACL。

MSR 系列路由器各款型对于本节所描述的命令及参数的支持情况有所不同，详细差异信息如下：

型号	命令	参数	描述
MSR 900	**acl**	*acl-number*	100～199：WLAN ACL 2000～2999：基本IPv4 ACL 3000～3999：高级IPv4 AC 4000～4999：二层ACL 5000～5999：用户自定义的ACL
MSR 930			2000～2999：基本IPv4 ACL 3000～3999：高级IPv4 AC 4000～4999：二层ACL 5000～5999：用户自定义的ACL
MSR 20-1X			100～199：WLAN ACL 2000～2999：基本IPv4 ACL 3000～3999：高级IPv4 AC 4000～4999：二层ACL 5000～5999：用户自定义的ACL
MSR 20			
MSR 30			

型号	命令	参数	描述
MSR 50			100～199：WLAN ACL 2000～2999：基本IPv4 ACL 3000～3999：高级IPv4 AC 4000～4999：二层ACL 5000～5999：用户自定义的ACL MPU-G2不支持WLAN ACL
MSR 2600			100～199：WLAN ACL 2000～2999：基本IPv4 ACL 3000～3999：高级IPv4 AC 4000～4999：二层ACL 5000～5999：用户自定义的ACL

name *acl-name*：指定 ACL 的名称。*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 all。WLAN ACL 不支持本参数，即不允许为 WLAN ACL 设置名称

match-order { **auto** | **config** }：指定规则的匹配顺序，**auto** 表示按照自动排序（即“深度优先”原则）的顺序进行规则匹配，**config** 表示按照配置顺序进行规则匹配。缺省情况下，规则的匹配顺序为配置顺序。WLAN ACL 和用户自定义 ACL 都不支持本参数，它们的规则匹配顺序都只能为配置顺序。

all：指定全部 ACL（包括 WLAN ACL、IPv4 基本 ACL、IPv4 高级 ACL、二层 ACL 和用户自定义 ACL）。

【描述】

acl 命令用来创建一个 WLAN ACL、IPv4 基本 ACL、IPv4 高级 ACL、二层 ACL 或用户自定义 ACL，并进入相应的 ACL 视图。**undo acl** 命令用来删除指定或全部 ACL（包括 WLAN ACL、IPv4 基本 ACL、IPv4 高级 ACL、二层 ACL 和用户自定义 ACL）。

缺省情况下，不存在任何 ACL。

需要注意的是：

- 使用 **acl** 命令时，如果指定编号的 ACL 不存在，则创建该 ACL 并进入其视图，否则直接进入其视图。
- ACL 的名称只能在创建时设置。ACL 一旦创建，便不允许再修改或删除其原有名称。
- 当 ACL 内不存在任何规则时，用户可以使用本命令对该 ACL 的规则匹配顺序进行修改，否则不允许进行修改。

相关配置可参考命令 **display acl**。

【举例】

创建一个编号为 2000 的 IPv4 基本 ACL，并进入其视图。

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000]
```

创建一个编号为 2001 的 IPv4 基本 ACL，指定其名称为 flow，并进入其视图。

```
<Sysname> system-view
[Sysname] acl number 2001 name flow
[Sysname-acl-basic-2001-flow]
```

1.1.2 acl copy

【命令】

acl copy { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

source-acl-number：指定源 ACL 的编号，该 ACL 必须存在。本参数的取值范围及其代表的 ACL 类型如下：

- 100～199：表示 WLAN ACL；
- 2000～2999：表示 IPv4 基本 ACL；
- 3000～3999：表示 IPv4 高级 ACL；
- 4000～4999：表示二层 ACL；
- 5000～5999：表示用户自定义 ACL。

name *source-acl-name*：指定源 ACL 的名称，该 ACL 必须存在。*source-acl-name* 为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。WLAN ACL 不支持本参数，即不允许为 WLAN ACL 设置名称。

dest-acl-number：指定目的 ACL 的编号，该 ACL 必须不存在。若未指定本参数，系统将为目的 ACL 自动分配一个与源 ACL 类型相同且可用的最小编号。本参数的取值范围及其代表的 ACL 类型如下：

- 100～199：表示 WLAN ACL；
- 2000～2999：表示 IPv4 基本 ACL；
- 3000～3999：表示 IPv4 高级 ACL；
- 4000～4999：表示二层 ACL；
- 5000～5999：表示用户自定义 ACL。

MSR 系列路由器各款型对于本节所描述的命令及参数的支持情况有所不同，详细差异信息如下：

型号	命令	参数	描述
MSR 900	**acl copy**	*acl-number*	100～199：WLAN ACL 2000～2999：基本IPv4 ACL 3000～3999：高级IPv4 AC 4000～4999：二层ACL 5000～5999：用户自定义的ACL

型号	命令	参数	描述
MSR 930			2000～2999：基本IPv4 ACL 3000～3999：高级IPv4 AC 4000～4999：二层ACL 5000～5999：用户自定义的ACL
MSR 20-1X			100～199：WLAN ACL 2000～2999：基本IPv4 ACL 3000～3999：高级IPv4 AC 4000～4999：二层ACL 5000～5999：用户自定义的ACL
MSR 20			
MSR 30			
MSR 50			100～199：WLAN ACL 2000～2999：基本IPv4 ACL 3000～3999：高级IPv4 AC 4000～4999：二层ACL 5000～5999：用户自定义的ACL MPU-G2不支持WLAN ACL
MSR 2600			100～199：WLAN ACL 2000～2999：基本IPv4 ACL 3000～3999：高级IPv4 AC 4000～4999：二层ACL 5000～5999：用户自定义的ACL

name *dest-acl-name*：指定目的 ACL 的名称，该 ACL 必须不存在。*dest-acl-name* 为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 all。WLAN ACL 不支持本参数，即不允许为 WLAN ACL 设置名称。若未指定本参数，系统将不会为目的 ACL 设置名称。

【描述】

acl copy 命令用来复制并生成新的 WLAN ACL、IPv4 基本 ACL、IPv4 高级 ACL、二层 ACL 或用户自定义 ACL。

需要注意的是：

- 目的 ACL 的类型要与源 ACL 的类型相同。
- 目的 ACL 的名称只能在复制时设置。且目的 ACL 一旦生成，便不允许再修改或删除其原有名称。
- 除了 ACL 的编号和名称不同外，新生成的 ACL（即目的 ACL）的匹配顺序、规则匹配统计功能的使能情况、规则编号的步长、所包含的规则、规则的描述信息以及 ACL 的描述信息等都与源 ACL 的相同。

【举例】

通过复制已存在的 IPv4 基本 ACL 2001，来生成一个新的编号为 2002 的同类型 ACL。

```
<Sysname> system-view
[Sysname] acl copy 2001 to 2002
```

1.1.3 acl ipv6

【命令】

acl ipv6 number *acl6-number* [**name** *acl6-name*] [**match-order** { **auto** | **config** }]

undo acl ipv6 { **all** | **name** *acl6-name* | **number** *acl6-number* }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

number *acl6-number*：指定 ACL 的编号。*acl6-number* 表示 ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000～2999：表示 IPv6 基本 ACL；
- 3000～3999：表示 IPv6 高级 ACL；
- 10000～42767：表示简单 ACL。

name *acl6-name*：指定 ACL 的名称。*acl6-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 all。简单 ACL 不支持本参数，即不允许为简单 ACL 设置名称。

match-order { **auto** | **config** }：指定规则的匹配顺序，**auto** 表示按照自动排序（即“深度优先”原则）的顺序进行规则匹配，**config** 表示按照配置顺序进行规则匹配。缺省情况下，规则的匹配顺序为配置顺序。简单 ACL 不支持本参数，因为简单 ACL 只能包含一条规则，因此不存在匹配顺序的问题。

all：指定全部 ACL（包括 IPv6 基本 ACL、IPv6 高级 ACL 和简单 ACL）。

【描述】

acl ipv6 命令用来创建一个 IPv6 基本 ACL、IPv6 高级 ACL 或简单 ACL，并进入相应的 ACL 视图。**undo acl ipv6** 命令用来删除指定或全部 ACL（包括 IPv6 基本 ACL、IPv6 高级 ACL 和简单 ACL）。

缺省情况下，不存在任何 ACL。

需要注意的是：

- 使用 **acl ipv6** 命令时，如果指定编号的 ACL 不存在，则创建该 ACL 并进入其视图，否则直接进入其视图。
- ACL 的名称只能在创建时设置。ACL 一旦创建，便不允许再修改或删除其原有名称。
- 当 ACL 内不存在任何规则时，用户可以使用本命令对该 ACL 的规则匹配顺序进行修改，否则不允许进行修改。

相关配置可参考命令 **display acl ipv6**。

【举例】

创建一个编号为 2000 的 IPv6 基本 ACL，并进入其视图。

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000]
```

创建一个编号为 2001 的 IPv6 基本 ACL，指定其名称为 flow，并进入其视图。

```
<Sysname> system-view
[Sysname] acl ipv6 number 2001 name flow
[Sysname-acl6-basic-2001-flow]
```

1.1.4 acl ipv6 copy

【命令】

acl ipv6 copy { *source-acl6-number* | **name** *source-acl6-name* } **to** { *dest-acl6-number* | **name** *dest-acl6-name* }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

source-acl6-number：指定源 ACL 的编号，该 ACL 必须存在。本参数的取值范围及其代表的 ACL 类型如下：

- 2000～2999：表示 IPv6 基本 ACL；
- 3000～3999：表示 IPv6 高级 ACL。

name *source-acl6-name*：指定源 ACL 的名称，该 ACL 必须存在。*source-acl6-name* 为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。

dest-acl6-number：指定目的 ACL 的编号，该 ACL 必须不存在。若未指定本参数，系统将为目的 ACL 自动分配一个与源 ACL 类型相同且可用的最小编号。本参数的取值范围及其代表的 ACL 类型如下：

- 2000～2999：表示 IPv6 基本 ACL；
- 3000～3999：表示 IPv6 高级 ACL。

name *dest-acl6-name*：指定目的 ACL 的名称，该 ACL 必须不存在。*dest-acl6-name* 为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 all。若未指定本参数，系统将不会为目的 ACL 设置名称。

【描述】

acl ipv6 copy 命令用来复制并生成新的 IPv6 基本 ACL 或 IPv6 高级 ACL。

需要注意的是：

- 目的 ACL 的类型要与源 ACL 的类型相同。
- 目的 ACL 的名称只能在复制时设置。目的 ACL 一旦生成，便不允许再修改或删除其原有名称。
- 除了 ACL 的编号和名称不同外，新生成的目的 ACL 的匹配顺序、规则匹配统计功能的使能情况、规则编号的步长、所包含的规则、规则的描述信息以及 ACL 的描述信息等都与源 ACL 的相同。

【举例】

通过复制已存在的 IPv6 基本 ACL 2001，来生成一个新的编号为 2002 的同类型 ACL。

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

```
[Sysname] acl ipv6 copy 2001 to 2002
```

1.1.5 acl ipv6 name

【命令】

acl ipv6 name *acl6-name*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

acl6-name：指定 IPv6 基本 ACL 或 IPv6 高级 ACL 的名称，该 ACL 必须存在。为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。

【描述】

acl ipv6 name 命令用来进入指定名称的 IPv6 基本 ACL 或 IPv6 高级 ACL 视图。

相关配置可参考命令 **acl ipv6**。

【举例】

进入名称为 flow 的 IPv6 基本 ACL 的视图。

```
<Sysname> system-view
[Sysname] acl ipv6 name flow
[Sysname-acl6-basic-2001-flow]
```

1.1.6 acl name

【命令】

acl name *acl-name*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

acl-name：指定 IPv4 基本 ACL、IPv4 高级 ACL、二层 ACL 或用户自定义 ACL 的名称，该 ACL 必须存在。本参数为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。

【描述】

acl name 命令用来进入指定名称的 IPv4 基本 ACL、IPv4 高级 ACL、二层 ACL 或用户自定义 ACL 视图。

相关配置可参考命令 **acl**。

【举例】

进入名称为 flow 的 IPv4 基本 ACL 的视图。

```
<Sysname> system-view
[Sysname] acl name flow
[Sysname-acl-basic-2001-flow]
```

1.1.7 description

【命令】

description *text*

undo description

【视图】

WLAN ACL 视图/IPv4 基本 ACL 视图/IPv4 高级 ACL 视图/IPv6 基本 ACL 视图/IPv6 高级 ACL 视图/二层 ACL 视图/用户自定义 ACL 视图/简单 ACL 视图

【缺省级别】

2：系统级

【参数】

text：表示 ACL 的描述信息，为 1～127 个字符的字符串，区分大小写。

【描述】

description 命令用来配置 ACL 的描述信息。**undo description** 命令用来删除 ACL 的描述信息。

缺省情况下，ACL 没有任何描述信息。

相关配置可参考命令 **display acl** 和 **display acl ipv6**。

注意

MSR 50 路由器的 MPU-G2 主控板和 MSR 930 路由器不支持 WLAN ACL 视图。

【举例】

为 IPv4 基本 ACL 2000 配置描述信息。

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] description This is an IPv4 basic ACL.
```

为 IPv6 基本 ACL 2000 配置描述信息。

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] description This is an IPv6 basic ACL.
```

1.1.8 display acl

【命令】

display acl { *acl-number* | **all** | **name** *acl-name* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

acl-number：显示指定编号的 ACL 的配置和运行情况。*acl-number* 表示 ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 100～199：表示 WLAN ACL；
- 2000～2999：表示 IPv4 基本 ACL；
- 3000～3999：表示 IPv4 高级 ACL；
- 4000～4999：表示二层 ACL；
- 5000～5999：表示用户自定义 ACL。

MSR 系列路由器各款型对于本节所描述的命令及参数的支持情况有所不同，详细差异信息如下：

型号	命令	参数	描述
MSR 900	**display acl**	*acl-number*	100～199：WLAN ACL 2000～2999：基本IPv4 ACL 3000～3999：高级IPv4 AC 4000～4999：二层ACL 5000～5999：用户自定义的ACL
MSR 930			2000～2999：基本IPv4 ACL 3000～3999：高级IPv4 AC 4000～4999：二层ACL 5000～5999：用户自定义的ACL
MSR 20-1X			100～199：WLAN ACL 2000～2999：基本IPv4 ACL 3000～3999：高级IPv4 AC 4000～4999：二层ACL 5000～5999：用户自定义的ACL
MSR 20			
MSR 30			
MSR 50			100～199：WLAN ACL 2000～2999：基本IPv4 ACL 3000～3999：高级IPv4 AC 4000～4999：二层ACL 5000～5999：用户自定义的ACL MPU-G2不支持WLAN ACL
MSR 2600			100～199：WLAN ACL 2000～2999：基本IPv4 ACL 3000～3999：高级IPv4 AC 4000～4999：二层ACL 5000～5999：用户自定义的ACL

all：显示全部 ACL（包括 WLAN ACL、IPv4 基本 ACL、IPv4 高级 ACL、二层 ACL 和用户自定义 ACL）的配置和运行情况。

name *acl-name*：显示指定名称的 ACL 的配置和运行情况。*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display acl 命令用来显示指定或全部 ACL（包括 WLAN ACL、IPv4 基本 ACL、IPv4 高级 ACL、二层 ACL 和用户自定义 ACL）的配置和运行情况。

需要注意的是，本命令将按照实际匹配顺序来排列 ACL 内的规则，即：当 ACL 的规则匹配顺序为配置顺序时，各规则将按照编号由小到大排列；当 ACL 的规则匹配顺序为自动排序时，各规则将按照“深度优先”原则由深到浅排列。

【举例】

显示全部 ACL（包括 WLAN ACL、IPv4 基本 ACL、IPv4 高级 ACL、二层 ACL 和用户自定义 ACL）的配置和运行情况。

```
<Sysname> display acl all
Basic ACL  2000, named flow, 3 rules,
This is an IPv4 basic ACL.
Statistics is enabled
ACL's step is 5
 rule 0 permit
 rule 5 permit source 1.1.1.1 0 (2 times matched)
 rule 10 permit vpn-instance mk

Basic ACL  2001, named -none-, 3 rules, match-order is auto,
ACL's step is 5
 rule 10 permit vpn-instance rd
 rule 10 comment This rule is used in VPN rd.
 rule 5 permit source 2.2.2.2 0
 rule 0 permit
```

表1-1 **display acl** 命令显示信息描述表

字段	描述
Basic ACL 2000	该ACL的类型和编号，ACL的类型包括： • WLAN ACL：表示 WLAN ACL • Basic ACL：表示 IPv4 基本 ACL • Advanced ACL：表示 IPv4 高级 ACL

字段	描述
	• Ethernet frame ACL：表示二层 ACL • User defined ACL：表示用户自定义 ACL
named flow	该ACL的名称为flow，-none-表示没有名称（WLAN ACL没有本字段）
3 rules	该ACL内包含的规则数量
match-order is auto	该ACL的规则匹配顺序为自动排序（匹配顺序为配置顺序时不显示本字段）
This is an IPv4 basic ACL.	该ACL的描述信息
ACL's step is 5	该ACL的规则编号的步长值为5
rule 0 permit	规则0的具体内容
2 times matched	该规则匹配的次数为2（仅统计软件ACL的匹配次数，当匹配次数为0时不显示本字段）
Uncompleted	该规则下发未完成，因此不会生效。这种情况通常是在ACL被动态修改之后，由于该规则的资源不足或硬件限制而导致其应用失败
rule 10 comment This rule is used in VPN rd.	规则10的描述信息

1.1.9 display acl ipv6

【命令】

display acl ipv6 { *acl6-number* | **all** | **name** *acl6-name* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

acl6-number：显示指定编号的 ACL 的配置和运行情况。*acl6-number* 表示 ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000～2999：表示 IPv6 基本 ACL；
- 3000～3999：表示 IPv6 高级 ACL；
- 10000～42767：表示简单 ACL。

all：显示全部 ACL（包括 IPv6 基本 ACL、IPv6 高级 ACL 和简单 ACL）的配置和运行情况。

name *acl6-name*：显示指定名称的 ACL 的配置和运行情况。*acl6-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display acl ipv6 命令用来显示指定或全部 ACL（包括 IPv6 基本 ACL、IPv6 高级 ACL 和简单 ACL）的配置和运行情况。

需要注意的是，本命令将按照实际匹配顺序来排列 ACL 内的规则，即：当 ACL 的规则匹配顺序为配置顺序时，各规则将按照编号由小到大排列；当 ACL 的规则匹配顺序为自动排序时，各规则将按照“深度优先”原则由深到浅排列。

【举例】

显示全部 ACL（包括 IPv6 基本 ACL、IPv6 高级 ACL 和简单 ACL）的配置和运行情况。

```
<Sysname> display acl ipv6 all
 Basic IPv6 ACL  2000, named flow, 3 rules,
 This is an IPv6 basic ACL.
 Statistics is enabled
 ACL's step is 5
 rule 0 permit
 rule 5 permit source 1::/64 (2 times matched)
 rule 10 permit vpn-instance mk

 Basic IPv6 ACL  2001, named -none-, 3 rules, match-order is auto,
 ACL's step is 5
 rule 10 permit vpn-instance mk
 rule 10 comment This rule is used in VPN rd
 rule 5 permit source 1::/64
 rule 0 permit
```

表1-2 **display acl ipv6** 命令显示信息描述表

字段	描述
Basic IPv6 ACL 2000	该ACL的类型和编号，ACL的类型包括： • Basic IPv6 ACL：表示 IPv6 基本 ACL • Advanced IPv6 ACL：表示 IPv6 高级 ACL • Simple IPv6 ACL：表示简单 ACL
named flow	该ACL的名称为flow，-none-表示没有名称（简单ACL没有本字段）
3 rules	该ACL内包含的规则数量
match-order is auto	该ACL的规则匹配顺序为自动排序（匹配顺序为配置顺序时不显示本字段）
This is an IPv6 basic ACL.	该ACL的描述信息
ACL's step is 5	该ACL的规则编号的步长值为5
rule 0 permit	规则0的具体内容
2 times matched	该规则匹配的次数为5，仅统计软件ACL的匹配次数（匹配次数为0时不显示本字段）
Uncompleted	该规则下发未完成，因此不会生效。这种情况通常是在ACL被动态修改之后，由

字段	描述
	于该规则的资源不足或硬件限制而导致其应用失败
rule 10 comment This rule is used in VPN rd	规则10的描述信息

1.1.10 display time-range

【命令】

display time-range { *time-range-name* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

time-range-name：显示指定名称的时间段的配置和状态信息。*time-range-name* 表示时间段的名称，为 1～32 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。

all：显示所有时间段的配置和状态信息。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display time-range 命令用来显示时间段的配置和状态信息。

【举例】

显示时间段 t4 的配置和状态信息。

```
<Sysname> display time-range t4
Current time is 17:12:34 4/13/2010 Tuesday

Time-range : t4 ( Inactive )
 10:00 to 12:00 Mon
 14:00 to 16:00 Wed
 from 00:00 1/1/2010 to 00:00 2/1/2010
 from 00:00 6/1/2010 to 00:00 7/1/2010
```

表1-3 display time-range 命令显示信息描述表

字段	描述
Current time	系统当前的时间

字段	描述
Time-range	时间段的配置信息，包括： • 时间段的名称 • 时间段的状态，包括 Active（生效）和 Inactive（未生效）两种状态 • 时间段的时间范围

1.1.11 reset acl counter

【命令】

reset acl counter { *acl-number* | **all** | **name** *acl-name* }

【视图】

用户视图

【缺省级别】

2：系统级

【参数】

acl-number：指定 ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 100～199：表示 WLAN ACL；
- 2000～2999：表示 IPv4 基本 ACL；
- 3000～3999：表示 IPv4 高级 ACL；
- 4000～4999：表示二层 ACL；
- 5000～5999：表示用户自定义 ACL。

MSR 系列路由器各款型对于本节所描述的命令及参数的支持情况有所不同，详细差异信息如下：

型号	命令	参数	描述
MSR 900	**reset acl counter**	*acl-number*	100～199：WLAN ACL 2000～2999：基本IPv4 ACL 3000～3999：高级IPv4 AC 4000～4999：二层ACL 5000～5999：用户自定义的ACL
MSR 930			2000～2999：基本IPv4 ACL 3000～3999：高级IPv4 AC 4000～4999：二层ACL 5000～5999：用户自定义的ACL
MSR 20-1X			100～199：WLAN ACL 2000～2999：基本IPv4 ACL 3000～3999：高级IPv4 AC 4000～4999：二层ACL 5000～5999：用户自定义的ACL
MSR 20			
MSR 30			

型号	命令	参数	描述
MSR 50			100～199：WLAN ACL 2000～2999：基本IPv4 ACL 3000～3999：高级IPv4 AC 4000～4999：二层ACL 5000～5999：用户自定义的ACL MPU-G2不支持WLAN ACL
MSR 2600			100～199：WLAN ACL 2000～2999：基本IPv4 ACL 3000～3999：高级IPv4 AC 4000～4999：二层ACL 5000～5999：用户自定义的ACL

all：指定全部 ACL（包括 WLAN ACL、IPv4 基本 ACL、IPv4 高级 ACL、二层 ACL 和用户自定义 ACL）。

name *acl-name*：指定 ACL 的名称。*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。

【描述】

reset acl counter 命令用来清除指定或全部 ACL（包括 WLAN ACL、IPv4 基本 ACL、IPv4 高级 ACL、二层 ACL 和用户自定义 ACL）的统计信息。

相关配置可参考命令 **display acl**。

【举例】

清除编号为 2001 的 IPv4 基本 ACL 的统计信息。

```
<Sysname> reset acl counter 2001
```

1.1.12 reset acl ipv6 counter

【命令】

reset acl ipv6 counter { *acl6-number* | **all** | **name** *acl6-name* }

【视图】

用户视图

【缺省级别】

2：系统级

【参数】

acl6-number：指定 ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000～2999：表示 IPv6 基本 ACL；
- 3000～3999：表示 IPv6 高级 ACL。

all：指定全部 ACL（包括 IPv6 基本 ACL 和 IPv6 高级 ACL）。

name *acl6-name*：指定 ACL 的名称。*acl6-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。

【描述】

reset acl ipv6 counter 命令用来清除全部 ACL（包括 IPv6 基本 ACL 和 IPv6 高级 ACL）的统计信息。

相关配置可参考命令 **display acl ipv6**。

【举例】

清除编号为 2001 的 IPv6 基本 ACL 的统计信息。

```
<Sysname> reset acl ipv6 counter 2001
```

1.1.13 rule (Ethernet frame header ACL view)

【命令】

rule [*rule-id*] { **deny** | **permit** } [**cos** *vlan-pri* | **counting** | **dest-mac** *dest-address dest-mask* | **logging** | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *

undo rule *rule-id* [**counting** | **time-range**] *

【视图】

二层 ACL 视图

【缺省级别】

2：系统级

【参数】

rule-id：指定二层 ACL 规则的编号，取值范围为 0～65534。若未指定本参数，系统将按照步长从 0 开始，自动分配一个大于现有最大编号的最小编号。譬如现有规则的最大编号为 28，步长为 5，那么自动分配的新编号将是 30。

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

cos *vlan-pri*：指定 802.1p 优先级。*vlan-pri* 表示 802.1p 优先级，可输入的形式如下：

- 数字：取值范围为 0～7；
- 名称：**best-effort**、**background**、**spare**、**excellent-effort**、**controlled-load**、**video**、**voice** 和 **network-management**，依次对应于数字 0～7。

counting：表示使能本规则的匹配统计功能，缺省为关闭。

dest-mac *dest-addr dest-mask*：指定目的 MAC 地址范围。*dest-addr* 表示目的 MAC 地址，格式为 H-H-H。*dest-mask* 表示目的 MAC 地址的掩码，格式为 H-H-H。

logging：表示对符合条件的报文可记录日志信息。该功能需要使用该 ACL 的模块支持日志记录功能。

lsap *lsap-type lsap-type-mask*：指定 LLC 封装中的 DSAP 字段和 SSAP 字段。*lsap-type* 表示数据帧的封装格式，为 16 比特的十六进制数。*lsap-type-mask* 表示 LSAP 的类型掩码，为 16 比特的十六进制数，用于指定屏蔽位。

type *protocol-type protocol-type-mask*：指定链路层协议类型。*protocol-type* 表示 16 比特的十六进制数表征的数据帧类型，对应 Ethernet_II 类型和 Ethernet_SNAP 类型帧中的 type 域。*protocol-type-mask* 表示类型掩码，为 16 比特的十六进制数，用于指定屏蔽位。

source-mac *sour-addr source-mask*：指定源 MAC 地址范围。*sour-addr* 表示源 MAC 地址，格式为 H-H-H。*sour-mask* 表示源 MAC 地址的掩码，格式为 H-H-H。

time-range *time-range-name*：指定规则生效的时间段。*time-range-name* 表示时间段的名称，为 1～32 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。若该时间段尚未配置，该规则仍会成功创建但系统将给出提示信息，并在该时间段的配置完成后此规则才会生效。

【描述】

rule 命令用来为二层 ACL 创建一条规则。**undo rule** 命令用来为二层 ACL 删除一条规则或删除规则中的部分内容。

缺省情况下，二层 ACL 内不存在任何规则。

需要注意的是：

- 使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。
- 新创建或修改的规则不能与已有规则的内容完全相同，否则将提示出错，并导致该操作失败。
- 当 ACL 的规则匹配顺序为配置顺序时，允许修改该 ACL 内的任意一条已有规则；当 ACL 的规则匹配顺序为自动排序时，不允许修改该 ACL 内的已有规则，否则将提示出错。
- 使用 **undo rule** 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- 使用 **undo rule** 命令时必须指定一个已存在规则的编号，可以使用 **display acl all** 命令来查看所有已存在的规则。

相关配置可参考命令 **acl**、**display acl**、**step** 和 **time-range**。

【举例】

为二层 ACL 4000 创建规则如下：允许 ARP 报文通过，但拒绝 RARP 报文通过。

```
<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] rule permit type 0806 ffff
[Sysname-acl-ethernetframe-4000] rule deny type 8035 ffff
```

1.1.14 rule (IPv4 advanced ACL view)

【命令】

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* | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **logging** | **precedence** *precedence* | **source** { *source-address source-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name* | **tos** *tos* | **vpn-instance** *vpn-instance-name*] *

undo rule *rule-id* [{ { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **established** } | **counting** | **destination** | **destination-port** | **dscp** | **fragment** | **icmp-type** | **logging** | **precedence** | **source** | **source-port** | **time-range** | **tos** | **vpn-instance**] *

【视图】

IPv4 高级 ACL 视图

【缺省级别】

2：系统级

【参数】

rule-id：指定 IPv4 高级 ACL 规则的编号，取值范围为 0～65534。若未指定本参数，系统将按照步长从 0 开始，自动分配一个大于现有最大编号的最小编号。譬如现有规则的最大编号为 28，步长为 5，那么自动分配的新编号将是 30。

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

protocol：表示 IPv4 承载的协议类型，可输入的形式如下：

- 数字：取值范围为 0～255；
- 名称（括号内为对应的数字）：可选取 **gre**（47）、**icmp**（1）、**igmp**（2）、**ip**、**ipinip**（4）、**ospf**（89）、**tcp**（6）或 **udp**（17）。

*protocol*之后可配置如 表 1-4 所示的规则信息参数。

表1-4 规则信息参数

参数	类别	作用	说明
source { *sour-addr* *sour-wildcard* | **any** }	源地址	指定ACL规则的源地址信息	*source-address*：源IP地址 *source-wildcard*：源IP地址的通配符掩码（为0表示主机地址） **any**：任意源IP地址
destination { *dest-addr* *dest-wildcard* | **any** }	目的地址	指定ACL规则的目的地址信息	*dest-address*：目的IP地址 *dest-wildcard*：目的IP地址的通配符掩码（为0表示主机地址） **any**：任意目的IP地址
counting	统计	使能本规则的匹配统计功能，缺省为关闭	-
precedence *precedence*	报文优先级	IP优先级	*precedence*：用数字表示时，取值范围为0～7；用名称表示时，为**routine**、**priority**、**immediate**、**flash**、**flash-override**、**critical**、**internet**或**network**，分别对应于数字0～7
tos *tos*	报文优先级	ToS优先级	*tos*：用数字表示时，取值范围为0～15；用名称表示时，可选取**max-reliability**（2）、**max-throughput**（4）、**min-delay**（8）、**min-monetary-cost**（1）或**normal**（0）
dscp *dscp*	报文优先级	DSCP优先级	*dscp*：用数字表示时，取值范围为0～63；用名称表示时，可选取**af11**（10）、**af12**（12）、

参数	类别	作用	说明
			af13（14）、**af21**（18）、**af22**（20）、**af23**（22）、**af31**（26）、**af32**（28）、**af33**（30）、**af41**（34）、**af42**（36）、**af43**（38）、**cs1**（8）、**cs2**（16）、**cs3**（24）、**cs4**（32）、**cs5**（40）、**cs6**（48）、**cs7**（56）、**default**（0）或**ef**（46）
logging	日志操作	对符合条件的报文可记录日志信息	该功能需要使用该ACL的模块支持日志记录功能
vpn-instance *vpn-instance-name*	VPN实例	对指定VPN实例中的报文有效	*vpn-instance-name*：MPLS L3VPN的VPN实例名称，为1～31个字符的字符串，区分大小写 若未指定本参数，表示该规则仅对非VPN报文有效
fragment	报文分片	仅分片报文的非首个分片有效，而对非分片报文和分片报文的首个分片报文无效	若未指定本参数，表示该规则对所有报文（包括非分片报文和分片报文的每个分片）均有效
time-range *time-range-name*	时间段	指定规则生效的时间段	*time-range-name*：时间段的名称，为1～32个字符的字符串，不区分大小写，必须以英文字母a～z或A～Z开头。若该时间段尚未配置，该规则仍会成功创建但系统将给出提示信息，并在该时间段的配置完成后此规则才会生效

注意

如果指定参数 **dscp** 的同时还指定了参数 **precedence** 或 **tos**，那么对参数 **precedence** 和 **tos** 所作的配置将不会生效。

当*protocol*为**tcp**（6）或**udp**（17）时，用户还可配置如 表 1-5 所示的规则信息参数。

表1-5 TCP/UDP 特有的规则信息参数

参数	类别	作用	说明
source-port *operator port1* [*port2*]	源端口	定义TCP/UDP报文的源端口信息	*operator*：操作符，取值可以为**lt**（小于）、**gt**（大于）、**eq**（等于）、**neq**（不等于）或者**range**（在范围内，包括边界值）。只有**range**操作符需要两个端口号做操作数，其它操作符只需要一个端口号做操作数 *port1*/*port2*：TCP或UDP的端口号，用数字表示时，取值范围为0～65535；用名称表示时，TCP端口号可选取**chargen**（19）、**bgp**（179）、**cmd**（514）、**daytime**（13）、**discard**（9）、**domain**（53）、**echo**（7）、**exec**（512）、**finger**（79）、**ftp**（21）、**ftp-data**（20）、**gopher**（70）、**hostname**（101）、**irc**（194）、**klogin**（543）、**kshell**（544）、**login**（513）、**lpd**（515）、**nntp**（119）、**pop2**（109）、**pop3**（110）、**smtp**（25）、**sunrpc**（111）、**tacacs**（49）、**talk**（517）、**telnet**（23）、**time**（37）、**uucp**（540）、**whois**（43）或**www**（80）；UDP端口号可选取**biff**（512）、**bootpc**
destination-port *operator port1* [*port2*]	目的端口	定义TCP/UDP报文的目的端口信息	

参数	类别	作用	说明
			（68）、**bootps**（67）、**discard**（9）、**dns**（53）、**dnsix**（90）、**echo**（7）、**mobilip-ag**（434）、**mobilip-mn**（435）、**nameserver**（42）、**netbios-dgm**（138）、**netbios-ns**（137）、**netbios-ssn**（139）、**ntp**（123）、**rip**（520）、**snmp**（161）、**snmptrap**（162）、**sunrpc**（111）、**syslog**（514）、**tacacs-ds**（65）、**talk**（517）、**tftp**（69）、**time**（37）、**who**（513）或**xdmcp**（177）
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	TCP报文标识	定义对携带不同标志位（包括ACK、FIN、PSH、RST、SYN和URG六种）的TCP报文的处理规则	TCP协议特有的参数。表示匹配携带不同标志位的TCP报文，各*value*的取值可为0或1（0表示不携带此标志位，1表示携带此标志位） 一条规则中各标志位之间为“或”的关系。譬如：当配置为**ack** 0 **psh** 1时，匹配不携带ACK或携带PSH标志位的TCP报文为准
established	TCP连接建立标识	定义对TCP连接报文的处理规则	TCP协议特有的参数。表示匹配携带ACK或RST标志位的TCP连接报文

当*protocol*为**icmp**（1）时，用户还可配置如 表 1-6 所示的规则信息参数。

表1-6 ICMP 特有的规则信息参数

参数	类别	作用	说明
icmp-type { *icmp-type* [*icmp-code*] | *icmp-message* }	ICMP报文的消息类型和消息码	指定本规则中ICMP报文的消息类型和消息码信息	*icmp-type*：ICMP消息类型，取值范围为0～255 *icmp-code*：ICMP消息码，取值范围为0～255 *icmp-message*：ICMP消息名称。可输入的ICMP消息名称，及其与消息类型和消息码的对应关系如表 1-7所示

表1-7 ICMP 消息名称与消息类型和消息码的对应关系

ICMP 消息名称	ICMP 消息类型	ICMP 消息码
echo	8	0
echo-reply	0	0
fragmentneed-DFset	3	4
host-redirect	5	1
host-tos-redirect	5	3
host-unreachable	3	1
information-reply	16	0
information-request	15	0
net-redirect	5	0
net-tos-redirect	5	2
net-unreachable	3	0
parameter-problem	12	0

ICMP 消息名称	ICMP 消息类型	ICMP 消息码
port-unreachable	3	3
protocol-unreachable	3	2
reassembly-timeout	11	1
source-quench	4	0
source-route-failed	3	5
timestamp-reply	14	0
timestamp-request	13	0
ttl-exceeded	11	0

【描述】

rule 命令用来为 IPv4 高级 ACL 创建一条规则。**undo rule** 命令用来为 IPv4 高级 ACL 删除一条规则或删除规则中的部分内容。

缺省情况下，IPv4 高级 ACL 内不存在任何规则。

需要注意的是：

- 使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。
- 新创建或修改的规则不能与已有规则的内容完全相同，否则将提示出错，并导致该操作失败。
- 当 ACL 的规则匹配顺序为配置顺序时，允许修改该 ACL 内的任意一条已有规则；当 ACL 的规则匹配顺序为自动排序时，不允许修改该 ACL 内的已有规则，否则将提示出错。
- 使用 **undo rule** 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- 使用 **undo rule** 命令时必须指定一个已存在规则的编号，可以使用 **display acl all** 命令来查看所有已存在的规则。

相关配置可参考命令 **acl**、**display acl**、**step** 和 **time-range**。

【举例】

为 IPv4 高级 ACL 3000 创建规则如下：允许 129.9.0.0/16 网段内的主机与 202.38.160.0/24 网段内主机的 WWW 端口（端口号为 80）建立连接，并对符合此条件的行为记录日志。

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule permit tcp source 129.9.0.0 0.0.255.255 destination 202.38.160.0
0.0.0.255 destination-port eq 80 logging
```

为 IPv4 高级 ACL 3001 创建规则如下：允许 IP 报文通过，但拒绝发往 192.168.1.0/24 网段的 ICMP 报文通过。

```
<Sysname> system-view
[Sysname] acl number 3001
[Sysname-acl-adv-3001] rule permit ip
[Sysname-acl-adv-3001] rule deny icmp destination 192.168.1.0 0.0.0.255
```

为 IPv4 高级 ACL 3002 创建规则如下：在出、入双方向上都允许建立 FTP 连接并传输 FTP 数据。

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

```
[Sysname] acl number 3002
[Sysname-acl-adv-3002] rule permit tcp source-port eq ftp
[Sysname-acl-adv-3002] rule permit tcp source-port eq ftp-data
[Sysname-acl-adv-3002] rule permit tcp destination-port eq ftp
[Sysname-acl-adv-3002] rule permit tcp destination-port eq ftp-data
```

为 IPv4 高级 ACL 3003 创建规则如下：在出、入双方向上都允许 SNMP 报文和 SNMP Trap 报文通过。

```
<Sysname> system-view
[Sysname] acl number 3003
[Sysname-acl-adv-3003] rule permit udp source-port eq snmp
[Sysname-acl-adv-3003] rule permit udp source-port eq snmptrap
[Sysname-acl-adv-3003] rule permit udp destination-port eq snmp
[Sysname-acl-adv-3003] rule permit udp destination-port eq snmptrap
```

1.1.15 rule (IPv4 basic ACL view)

【命令】

rule [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

undo rule *rule-id* [**counting** | **fragment** | **logging** | **source** | **time-range** | **vpn-instance**] *

【视图】

IPv4 基本 ACL 视图

【缺省级别】

2：系统级

【参数】

rule-id：指定 IPv4 基本 ACL 规则的编号，取值范围为 0～65534。若未指定本参数，系统将按照步长从 0 开始，自动分配一个大于现有最大编号的最小编号。譬如现有规则的最大编号为 28，步长为 5，那么自动分配的新编号将是 30。

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

counting：表示使能本规则的匹配统计功能，缺省为关闭。

fragment：表示仅对非首片分片报文有效，而对非分片报文和首片分片报文无效。若未指定本参数，表示该规则对非分片报文和分片报文均有效。

logging：表示对符合条件的报文可记录日志信息。该功能需要使用该 ACL 的模块支持日志记录功能。

source { *sour-addr sour-wildcard* | **any** }：指定规则的源地址信息。*sour-addr* 表示报文的源 IP 地址，*sour-wildcard* 表示源 IP 地址的通配符掩码（为 0 表示主机地址），**any** 表示任意源 IP 地址。

time-range *time-range-name*：指定规则生效的时间段。*time-range-name* 表示时间段的名称，为 1～32 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。若该时间段尚未配置，该规则仍会成功创建但系统将给出提示信息，并在该时间段的配置完成后此规则才会生效。

vpn-instance *vpn-instance-name*：表示对指定 VPN 实例中的报文有效。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。若未指定本参数，表示该规则仅对非 VPN 报文有效。

【描述】

rule 命令用来为 IPv4 基本 ACL 创建一条规则。**undo rule** 命令用来为 IPv4 基本 ACL 删除一条规则或删除规则中的部分内容。

缺省情况下，IPv4 基本 ACL 内不存在任何规则。

需要注意的是：

- 使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。
- 新创建或修改的规则不能与已有规则的内容完全相同，否则将提示出错，并导致该操作失败。
- 当 ACL 的规则匹配顺序为配置顺序时，允许修改该 ACL 内的任意一条已有规则；当 ACL 的规则匹配顺序为自动排序时，不允许修改该 ACL 内的已有规则，否则将提示出错。
- 使用 **undo rule** 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- 使用 **undo rule** 命令时必须指定一个已存在规则的编号，可以使用 **display acl all** 命令来查看所有已存在的规则。

相关配置可参考命令 **acl**、**display acl**。**step** 和 **time-range**。

【举例】

为 IPv4 基本 ACL 2000 创建规则如下：仅允许来自 10.0.0.0/8、172.17.0.0/16 和 192.168.1.0/24 网段的报文通过，而拒绝来自所有其它网段的报文通过。

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.0.0.0 0.255.255.255
[Sysname-acl-basic-2000] rule permit source 172.17.0.0 0.0.255.255
[Sysname-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Sysname-acl-basic-2000] rule deny source any
```

1.1.16 rule (IPv6 advanced ACL view)

【命令】

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*] | **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*] *

undo rule *rule-id* [{ { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **established** } | **counting** | **destination** | **destination-port** | **dscp** | **flow-label** | **fragment** | **icmp6-type** | **logging** | **routing** | **source** | **source-port** | **time-range** | **vpn-instance**] *

【视图】

IPv6 高级 ACL 视图

【缺省级别】

2：系统级

【参数】

rule-id：指定 IPv6 高级 ACL 规则的编号，取值范围为 0～65534。若未指定本参数，系统将按照步长从 0 开始，自动分配一个大于现有最大编号的最小编号。譬如现有规则的最大编号为 28，步长为 5，那么自动分配的新编号将是 30。

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

protocol：表示 IPv6 承载的协议类型，可输入的形式如下：

- 数字：取值范围为 0～255；
- 名称（括号内为对应的数字）：可选取 **gre**（47）、**icmpv6**（58）、**ipv6**、**ipv6-ah**（51）、**ipv6-esp**（50）、**ospf**（89）、**tcp**（6）或 **udp**（17）。

*protocol*之后可配置如 表 1-8 所示的规则信息参数。

表1-8 规则信息参数

参数	类别	作用	说明
source { *source-address source-prefix* | *source-address /source-prefix* | **any** }	源IPv6地址	指定ACL规则的源IPv6地址信息	*source-address*：源IPv6地址 *source-prefix*：源IP地址的前缀长度，取值范围1～128 **any**：任意源IPv6地址
destination { *dest-address dest-prefix* | *dest-address /dest-prefix* | **any** }	目的IPv6地址	指定ACL规则的目的IPv6地址信息	*dest-address*：目的IPv6地址 *dest-prefix*：目的IP地址的前缀长度，取值范围1～128 **any**：任意目的IPv6地址
counting	统计	使能本规则的匹配统计功能，缺省为关闭	-
dscp *dscp*	报文优先级	DSCP优先级	*dscp*：用数字表示时，取值范围为0～63；用名称表示时，可选取**af11**（10）、**af12**（12）、**af13**（14）、**af21**（18）、**af22**（20）、**af23**（22）、**af31**（26）、**af32**（28）、**af33**（30）、**af41**（34）、**af42**（36）、**af43**（38）、**cs1**（8）、**cs2**（16）、**cs3**（24）、**cs4**（32）、**cs5**（40）、**cs6**（48）、**cs7**（56）、**default**（0）或**ef**（46）
flow-label *flow-label-value*	流标签字段	指定IPv6基本报文头中流标签字段的值	*flow-label-value*：流标签字段的值，取值范围为0～1048575
logging	日志操作	对符合条件的报文可记录日志信息	该功能需要使用该ACL的模块支持日志记录功能
routing [**type** *routing-type*]	路由头	指定路由头的类型	*routing-type*：路由头类型的值，取值范围为0～255

参数	类别	作用	说明
			若指定了**type** *routing-type*参数，表示仅对指定类型的路由头有效；否则，表示对所有类型的路由头都有效
vpn-instance *vpn-instance-name*	VPN实例	对指定VPN实例中的报文有效	*vpn-instance-name*：MPLS L3VPN的VPN实例名称，为1～31个字符的字符串，区分大小写 若未指定本参数，表示该规则仅对非VPN报文有效
fragment	报文分片	仅对分片报文的非首个分片有效，而对非分片报文和分片报文的首个分片无效	若未指定本参数，表示该规则对所有报文（包括非分片报文和分片报文的每个分片）均有效
time-range *time-range-name*	时间段	指定规则生效的时间段	*time-range-name*：时间段的名称，为1～32个字符的字符串，不区分大小写，必须以英文字母a～z或A～Z开头。若该时间段尚未配置，该规则仍会成功创建但系统将给出提示信息，并在该时间段的配置完成后此规则才会生效

当*protocol*为**tcp**（6）或**udp**（17）时，用户还可配置如 表 1-9 所示的规则信息参数。

表1-9 TCP/UDP 特有的规则信息参数

参数	类别	作用	说明
source-port *operator port1* [*port2*]	源端口	定义TCP/UDP报文的源端口信息	*operator*：操作符，取值可以为**lt**（小于）、**gt**（大于）、**eq**（等于）、**neq**（不等于）或者**range**（在范围内，包括边界值）。只有**range**操作符需要两个端口号做操作数，其它操作符只需要一个端口号做操作数 *port1*/*port2*：TCP或UDP的端口号，用数字表示时，取值范围为0～65535；用名称表示时，TCP端口号可选取**chargen**（19）、**bgp**（179）、**cmd**（514）、**daytime**（13）、**discard**（9）、**domain**（53）、**echo**（7）、**exec**（512）、**finger**（79）、**ftp**（21）、**ftp-data**（20）、**gopher**（70）、**hostname**（101）、**irc**（194）、**klogin**（543）、**kshell**（544）、**login**（513）、**lpd**（515）、**nntp**（119）、**pop2**（109）、**pop3**（110）、**smtp**（25）、**sunrpc**（111）、**tacacs**（49）、**talk**（517）、**telnet**（23）、**time**（37）、**uucp**（540）、**whois**（43）或**www**（80）；UDP端口号可选取**biff**（512）、**bootpc**（68）、**bootps**（67）、**discard**（9）、**dns**（53）、**dnsix**（90）、**echo**（7）、**mobilip-ag**（434）、**mobilip-mn**（435）、**nameserver**（42）、**netbios-dgm**（138）、**netbios-ns**（137）、**netbios-ssn**（139）、**ntp**（123）、**rip**（520）、**snmp**（161）、**snmptrap**（162）、**sunrpc**（111）、**syslog**（514）、**tacacs-ds**（65）、**talk**（517）、**tftp**（69）、**time**（37）、**who**（513）或**xdmcp**（177）
destination-port *operator port1* [*port2*]	目的端口	定义TCP/UDP报文的目的端口信息	
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg**	TCP报文标识	定义对携带不同标志位（包括ACK、FIN、PSH、RST、SYN和URG六种）的TCP报文的处理	TCP协议特有的参数。表示匹配携带不同标志位的TCP报文，各*value*的取值可为0或1（0表示不携带此标志位，1表示携带此标志位） 一条规则中各标志位之间为“或”的关系。譬如：当配置为**ack** 0 **psh** 1时，匹配不携带ACK或携带PSH标志位

参数	类别	作用	说明
urg-value } *		规则	的TCP报文为准
established	TCP连接建立标识	定义对TCP连接报文的处理规则	TCP协议特有的参数。表示匹配携带ACK或RST标志位的TCP连接报文

当*protocol*为**icmpv6**（58）时，用户还可配置如 表 1-10 所示的规则信息参数。

表1-10 ICMPv6 特有的规则信息参数

参数	类别	作用	说明
icmp6-type { *icmp6-type* *icmp6-code* | *icmp6-message* }	ICMPv6报文的消息类型和消息码	指定本规则中ICMPv6报文的消息类型和消息码信息	*icmp6-type*：ICMPv6消息类型，取值范围为0～255 *icmp6-code*：ICMPv6消息码，取值范围为0～255 *icmp6-message*：ICMPv6消息名称。可以输入的ICMPv6消息名称，及其与消息类型和消息码的对应关系如表1-11所示

表1-11 ICMPv6 消息名称与消息类型和消息码的对应关系

ICMPv6 消息名称	ICMPv6 消息类型	ICMPv6 消息码
echo-reply	129	0
echo-request	128	0
err-Header-field	4	0
frag-time-exceeded	3	1
hop-limit-exceeded	3	0
host-admin-prohib	1	1
host-unreachable	1	3
neighbor-advertisement	136	0
neighbor-solicitation	135	0
network-unreachable	1	0
packet-too-big	2	0
port-unreachable	1	4
redirect	137	0
router-advertisement	134	0
router-solicitation	133	0
unknown-ipv6-opt	4	2
unknown-next-hdr	4	1

【描述】

rule 命令用来为 IPv6 高级 ACL 创建一条规则。**undo rule** 命令用来为 IPv6 高级 ACL 删除一条规则或删除规则中的部分内容。

缺省情况下，IPv6 高级 ACL 内不存在任何规则。

需要注意的是：

- 使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。
- 新创建或修改的规则不能与已有规则的内容完全相同，否则将提示出错，并导致该操作失败。
- 当 ACL 的规则匹配顺序为配置顺序时，允许修改该 ACL 内的任意一条已有规则；当 ACL 的规则匹配顺序为自动排序时，不允许修改该 ACL 内的已有规则，否则将提示出错。
- 使用 undo rule 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- 使用 undo rule 命令时必须指定一个已存在规则的编号，可以使用 display acl ipv6 all 命令来查看所有已存在的规则。

相关配置可参考命令 **acl ipv6**、**display ipv6 acl**、**step** 和 **time-range**。

【举例】

为 IPv6 高级 ACL 3000 创建规则如下：允许 2030:5060::/64 网段内的主机与 FE80:5060::/96 网段内主机的 WWW 端口（端口号为 80）建立连接，并对符合此条件的行为记录日志。

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule permit tcp source 2030:5060::/64 destination fe80:5060::/96
destination-port eq 80 logging
```

为 IPv6 高级 ACL 3001 创建规则如下：允许 IPv6 报文通过，但拒绝发往 FE80:5060:1001::/48 网段的 ICMPv6 报文通过。

```
<Sysname> system-view
[Sysname] acl ipv6 number 3001
[Sysname-acl6-adv-3001] rule permit ipv6
[Sysname-acl6-adv-3001] rule deny icmpv6 destination fe80:5060:1001:: 48
```

为 IPv6 高级 ACL 3002 创建规则如下：在出、入双方向上都允许建立 FTP 连接并传输 FTP 数据。

```
<Sysname> system-view
[Sysname] acl ipv6 number 3002
[Sysname-acl6-adv-3002] rule permit tcp source-port eq ftp
[Sysname-acl6-adv-3002] rule permit tcp source-port eq ftp-data
[Sysname-acl6-adv-3002] rule permit tcp destination-port eq ftp
[Sysname-acl6-adv-3002] rule permit tcp destination-port eq ftp-data
```

为 IPv6 高级 ACL 3003 创建规则如下：在出、入双方向上都允许 SNMP 报文和 SNMP Trap 报文通过。

```
<Sysname> system-view
[Sysname] acl ipv6 number 3003
[Sysname-acl6-adv-3003] rule permit udp source-port eq snmp
[Sysname-acl6-adv-3003] rule permit udp source-port eq snmptrap
[Sysname-acl6-adv-3003] rule permit udp destination-port eq snmp
[Sysname-acl6-adv-3003] rule permit udp destination-port eq snmptrap
```

1.1.17 rule (IPv6 basic ACL view)

【命令】

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*] *

undo rule *rule-id* [**counting** | **fragment** | **logging** | **routing** | **source** | **time-range** | **vpn-instance**] *

【视图】

IPv6 基本 ACL 视图

【缺省级别】

2：系统级

【参数】

rule-id：指定 IPv6 基本 ACL 规则的编号，取值范围为 0～65534。若未指定本参数，系统将按照步长从 0 开始，自动分配一个大于现有最大编号的最小编号。譬如现有规则的最大编号为 28，步长为 5，那么自动分配的新编号将是 30。

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

counting：表示使能本规则的匹配统计功能，缺省为关闭。

fragment：表示仅对非首片分片报文有效，而对非分片报文和首片分片报文无效。若未指定本参数，表示该规则对非分片报文和分片报文均有效。

logging：表示对符合条件的报文可记录日志信息。该功能需要使用该 ACL 的模块支持日志记录功能。

routing [**type** *routing-type*]：表示对所有或指定类型的路由头有效，*routing-type* 表示路由头类型的值，取值范围为 0～255。若指定了 **type** *routing-type* 参数，表示仅对指定类型的路由头有效；否则，表示对所有类型的路由头都有效。

source { *source-address source-prefix* | *source-address*/*source-prefix* | **any** }：指定规则的源 IPv6 地址信息。*source-address* 表示报文的源 IPv6 地址，*source-prefix* 表示源 IPv6 地址的前缀长度，取值范围为 1～128，**any** 表示任意源 IPv6 地址。

time-range *time-range-name*：指定规则生效的时间段。*time-range-name* 表示时间段的名称，为 1～32 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。若该时间段尚未配置，该规则仍会成功创建但系统将给出提示信息，并在该时间段的配置完成后此规则才会生效。

vpn-instance *vpn-instance-name*：表示对指定 VPN 实例中的报文有效。*vpn-instance-name* 表示 VPN 实例的名称，为 1～31 个字符的字符串，区分大小写。若未指定本参数，表示该规则仅对非 VPN 报文有效。

【描述】

rule 命令用来为 IPv6 基本 ACL 创建一条规则。**undo rule** 命令用来为 IPv6 基本 ACL 删除一条规则或删除规则中的部分内容。

缺省情况下，IPv6 基本 ACL 内不存在任何规则。

需要注意的是：

- 使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。
- 新创建或修改的规则不能与已有规则的内容完全相同，否则将提示出错，并导致该操作失败。
- 当 ACL 的规则匹配顺序为配置顺序时，允许修改该 ACL 内的任意一条已有规则；当 ACL 的规则匹配顺序为自动排序时，不允许修改该 ACL 内的已有规则，否则将提示出错。
- 使用 **undo rule** 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- 使用 **undo rule** 命令时必须指定一个已存在规则的编号，可以使用 **display acl ipv6 all** 命令来查看所有已存在的规则。

相关配置可参考命令 **acl ipv6**、**display ipv6 acl**、**step** 和 **time-range**。

【举例】

为 IPv6 基本 ACL 2000 创建规则如下：仅允许来自 1001::/16、3124:1123::/32 和 FE80:5060:1001::/48 网段的报文通过，而拒绝来自所有其它网段的报文通过。

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source 1001:: 16
[Sysname-acl6-basic-2000] rule permit source 3124:1123:: 32
[Sysname-acl6-basic-2000] rule permit source fe80:5060:1001:: 48
[Sysname-acl6-basic-2000] rule deny source any
```

1.1.18 rule (simple ACL view)

【命令】

rule *protocol* [**addr-flag** *addr-flag* | **destination** { *dest-address dest-prefix* | *dest-address /dest-prefix* | **any** } | **destination-port** *operator port1* [*port2*] | **dscp** *dscp* | **frag-type** { **fragment** | **fragment-subseq** | **non-fragment** | **non-subseq** } | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **source** { *source-address source-prefix* | *source-address /source-prefix* | **any** } | **source-port** *operator port1* [*port2*] | **tcp-type** { **tcpurg** | **tcpack** | **tcppsh** | **tcprst** | **tcpsyn** | **tcpfin** }] *

undo rule [**addr-flag** | **destination** | **destination-port** | **dscp** | **frag-type** | **icmp6-type** | **source** | **source-port** | **tcp-type**] *

【视图】

简单 ACL 视图

【缺省级别】

2：系统级

【参数】

protocol：表示 IPv6 承载的协议类型，可输入的形式如下：

- 数字：取值范围为 0～255，且数字前必须加关键字 **protocol**；
- 名称（括号内为对应的数字）：可选取 **gre**（47）、**icmpv6**（58）、**ipv6**、**ipv6-ah**（51）、**ipv6-esp**（50）、**ospf**（89）、**tcp**（6）或 **udp**（17）。

*protocol*之后可配置如 表 1-12 所示的规则信息参数。

表1-12 规则信息参数

参数	类别	作用	说明
addr-flag *addr-flag*	标志	指定源IPv6地址和目的IPv6地址联合模式	*addr-flag*：取值范围为1～6，各数字代表的地址联合模式如下： • 1：表示 64 位源地址前缀+64 位目的地址前缀 • 2：表示 64 位源地址前缀+64 位目的地址后缀 • 3：表示 64 位源地址后缀+64 位目的地址前缀 • 4：表示 64 位源地址后缀+64 位目的地址后缀 • 5：表示 128 位源地址 • 6：表示 128 位目的地址
source { *source-address source-prefix* | *source-address /source-prefix* | **any** }	源IPv6地址	指定ACL规则的源IPv6地址信息	*source-address*：源IPv6地址 *source-prefix*：源IPv6地址的前缀长度，取值范围1～128 **any**：任意源IPv6地址
destination { *dest-address dest-prefix* | *dest-address /dest-prefix* | **any** }	目的IPv6地址	指定ACL规则的目的IPv6地址信息	*dest*：目的IPv6地址 *dest-prefix*：目的IPv6地址的前缀长度，取值范围1～128 **any**：任意目的IPv6地址
frag-type { **fragment** | **fragment-subseq** | **non-fragment** | **non-subseq** }	报文分片标志	指定规则仅对哪些分片报文标志有效	**fragment**：仅对首片分片报文有效 **fragment-subseq**：仅对非首片分片报文有效 **non-fragment**：仅对非分片报文有效 **non-subseq**：仅对当前分片报文的最后一片有效
dscp *dscp*	报文优先级	指定DSCP优先级	*dscp*：取值范围为0～63

当*protocol*为**tcp**（6）或**udp**（17）时，用户还可配置如 表 1-13 所示的规则信息参数。

表1-13 TCP/UDP 特有的规则信息参数

参数	类别	作用	说明
source-port *operator port1* [*port2*]	源端口	指定TCP/UDP报文的源端口信息	*operator*：操作符，取值可以为**lt**（小于）、**gt**（大于）、**eq**（等于）或者**range**（在范围内，包括边界值）。只有**range**操作符需要两个端口号做操作数，其它操作符只需要一个端口号做操作数 *port1*/*port2*：TCP或UDP的端口号，用数字表示时，取值范围为0～65535；用名称表示时，TCP端口号可选取**chargen**（19）、**bgp**（179）、**cmd**（514）、**daytime**（13）、**discard**（9）、**domain**（53）、**echo**（7）、**exec**（512）、**finger**（79）、**ftp**（21）、**ftp-data**（20）、**gopher**（70）、**hostname**（101）、**irc**（194）、**klogin**（543）、**kshell**（544）、**login**（513）、**lpd**（515）、**nntp**（119）、**pop2**（109）、**pop3**（110）、**smtp**（25）、**sunrpc**（111）、**tacacs**（49）、**talk**（517）、**telnet**（23）、**time**（37）、**uucp**（540）、**whois**（43）或**www**（80）；UDP端口号可选取**biff**（512）、**bootpc**（68）、**bootps**（67）、**discard**（9）、**dns**（53）、**dnsix**（90）、
destination-port *operator port1* [*port2*]	目的端口	指定TCP/UDP报文的目的端口信息	

参数	类别	作用	说明
			echo（7）、**mobilip-ag**（434）、**mobilip-mn**（435）、**nameserver**（42）、**netbios-dgm**（138）、**netbios-ns**（137）、**netbios-ssn**（139）、**ntp**（123）、**rip**（520）、**snmp**（161）、**snmptrap**（162）、**sunrpc**（111）、**syslog**（514）、**tacacs-ds**（65）、**talk**（517）、**tftp**（69）、**time**（37）、**who**（513）或**xdmcp**（177）
tcp-type { **tcpurg** | **tcpack** | **tcppsh** | **tcprst** | **tcpsyn** | **tcpfin** }	TCP报文标志	指定TCP报文的标志	TCP协议特有的参数

当*protocol*为**icmpv6**（58）时，用户还可配置如 表 1-14 所示的规则信息参数。

表1-14 ICMPv6 特有的规则信息参数

参数	类别	作用	说明
icmp6-type { *icmp6-type* *icmp6-code* | *icmp6-message* }	ICMPv6报文的消息类型和消息码	指定规则中ICMPv6报文的消息类型和消息码信息	*icmp6-type*：ICMPv6消息类型，取值范围为0～255 *icmp6-code*：ICMPv6消息码，取值范围为0～255 *icmp6-message*：ICMPv6消息名称。可输入的ICMPv6消息名称，及其与消息类型和消息码的对应关系如表 1-15所示

表1-15 ICMPv6 消息名称与消息类型和消息码的对应关系

ICMPv6 消息名称	ICMPv6 消息类型	ICMPv6 消息码
echo-reply	129	0
echo-request	128	0
err-Header-field	4	0
frag-time-exceeded	3	1
hop-limit-exceeded	3	0
host-admin-prohib	1	1
host-unreachable	1	3
neighbor-advertisement	136	0
neighbor-solicitation	135	0
network-unreachable	1	0
packet-too-big	2	0
port-unreachable	1	4
redirect	137	0
router-advertisement	134	0
router-solicitation	133	0
unknown-ipv6-opt	4	2
unknown-next-hdr	4	1

【描述】

rule 命令用来为简单 ACL 创建规则。**undo rule** 命令用来为简单 ACL 删除规则或删除规则中的部分内容。

缺省情况下，简单 ACL 内不存在任何规则。

需要注意的是：

- 用 **rule** 命令时，如果不存在规则，则创建新的规则；如果已存在规则，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。
- 使用 **undo rule** 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。

相关配置可参考命令 **acl ipv6**。

【举例】

为简单 ACL 10000 创建规则，匹配来自 2200:100::/64 网段的带有 TCP RST 标志的 TCP 报文。

```
<Sysname> system-view
[Sysname] acl ipv6 number 10000
[Sysname-acl6-simple-10000] rule tcp addr-flag 4 source 2200:100::/64 tcp-type tcprst
```

1.1.19 rule (user-defined ACL view)

【命令】

rule [*rule-id*] { **deny** | **permit** } [**l2** *rule-string rule-mask offset* }&<1-8>] [**counting** | **time-range** *time-range-name*] *

undo rule *rule-id*

【视图】

用户自定义 ACL 视图

【缺省级别】

2：系统级

【参数】

rule-id：指定用户自定义 ACL 规则的编号，取值范围为 0～65534。若未指定本参数，系统将按照步长从 0 开始，自动分配一个大于现有最大编号的最小编号。譬如现有规则的最大编号为 28，步长为 5，那么自动分配的新编号将是 30。

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

l2：表示从 L2 帧头开始偏移。

rule-string：指定用户自定义的规则字符串，必须是 16 进制数组成，字符长度必须是偶数。

rule-mask：指定规则字符串的掩码，用于和报文作“与”操作，必须是 16 进制数组成，字符长度必须是偶数，且必须与 *rule-string* 的长度相同。

offset：指定偏移量，它以用户指定的报文头部为基准，指定从第几个字节开始进行比较。

&<1-8>：表示前面的参数最多可以输入 8 次。

counting：表示使能本规则的匹配统计功能，缺省为关闭。

time-range *time-range-name*：指定规则生效的时间段。*time-range-name* 表示时间段的名称，为1～32 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。若该时间段尚未配置，该规则仍会成功创建但系统将给出提示信息，并在该时间段的配置完成后此规则才会生效。

【描述】

rule 命令用来为用户自定义 ACL 创建一条规则。**undo rule** 命令用来为用户自定义 ACL 删除一条规则。

缺省情况下，用户自定义 ACL 内不存在任何规则。

需要注意的是：

- 使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。
- 新创建的规则不能与已有规则的内容完全相同，否则将提示出错，并导致创建失败。
- 使用 **undo rule** 命令时必须指定一个已存在规则的编号，可以使用 **display acl all** 命令来查看所有已存在的规则。

相关配置可参考命令 **acl**、**display acl** 和 **time-range**。

【举例】

为用户自定义 ACL 5005 创建一条规则，允许从 L2 帧头开始算起第 13、14 两字节的内容为 0x0806 的报文（即 ARP 报文）通过。

```
<Sysname> system-view
[Sysname] acl number 5005
[Sysname-acl-user-5005] rule permit l2 0806 ffff 12
```

1.1.20 rule (WLAN ACL view)

【命令】

rule [*rule-id*] { **deny** | **permit** } [**ssid** *ssid-name*]

undo rule *rule-id*

【视图】

WLAN ACL 视图

【缺省级别】

2：系统级

【参数】

rule-id：指定 WLAN ACL 规则的编号，取值范围为 0～65534。若未指定本参数，系统将按照步长从 0 开始，自动分配一个大于现有最大编号的最小编号。譬如现有规则的最大编号为 28，步长为 5，那么自动分配的新编号将是 30。

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

ssid *ssid-name*：指定 SSID（Service Set Identifier，服务集标识符）的名称，*ssid-name* 为 1～32 个字符的字符串，包括字母和数字，区分大小写，允许包含空格。若未指定本参数，表示该规则对所有 SSID 均有效。

【描述】

rule 命令用来为 WLAN ACL 创建一条规则。**undo rule** 命令用来为 WLAN ACL 删除一条规则。

缺省情况下，WLAN ACL 内不存在任何规则。

需要注意的是：

- 使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。
- 新创建或修改的规则不能与已有规则的内容完全相同，否则将提示出错，并导致该操作失败。
- 使用 **undo rule** 命令时必须指定一个已存在规则的编号，可以使用 **display acl all** 命令来查看所有已存在的规则。

相关配置可参考命令 **acl**、**display acl** 和 **step**。

MSR 系列路由器各款型对于本节所描述的命令及参数的支持情况有所不同，详细差异信息如下：

型号	命令	描述
MSR 900	**rule (WLAN ACL view)**	支持
MSR 930		不支持
MSR 20-1X		支持
MSR 20		支持
MSR 30		支持
MSR 50		支持（MPU-G2不支持）
MSR 2600		支持

【举例】

为 WLAN ACL 100 配置规则，允许 SSID 名称为 user1 的 WLAN 用户报文通过，并利用此规则应用于 VTY 用户 0 的访问权限。

```
<Sysname> system-view
[Sysname] acl number 100
[Sysname-acl-wlan-100] rule permit ssid user1
[Sysname-acl-wlan-100] quit
[Sysname] user-interface vty 0
[Sysname-ui-vty0] acl 100 inbound
```

1.1.21 rule comment

【命令】

rule *rule-id* **comment** *text*

undo rule *rule-id* **comment**

【视图】

WLAN ACL 视图/IPv4 基本 ACL 视图/IPv4 高级 ACL 视图/IPv6 基本 ACL 视图/IPv6 高级 ACL 视图/二层 ACL 视图/用户自定义 ACL 视图

MSR 系列路由器各款型对于本节所描述的命令及参数的支持情况有所不同，详细差异信息如下：

型号	命令	描述
MSR 900	WLAN ACL视图	支持
MSR 930		不支持
MSR 20-1X		支持
MSR 20		支持
MSR 30		支持
MSR 50		支持（MPU-G2不支持）
MSR 2600		支持

【缺省级别】

2：系统级

【参数】

rule-id：指定规则的编号，该规则必须存在。取值范围为 0～65534。

text：表示规则的描述信息，为 1～127 个字符的字符串，区分大小写。

【描述】

rule comment 命令用来为指定规则配置描述信息。**undo rule comment** 命令用来删除指定规则的描述信息。

缺省情况下，规则没有任何描述信息。

需要注意的是，使用 **rule comment** 命令时，如果指定的规则没有描述信息，则为其添加描述信息，否则修改其描述信息。

相关配置可参考命令 **display acl** 和 **display acl ipv6**。

【举例】

为 IPv4 基本 ACL 2000 配置规则 0，并为该规则配置描述信息。

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule 0 deny source 1.1.1.1 0
[Sysname-acl-basic-2000] rule 0 comment This rule is used on Ethernet 1/1.
```

为 IPv6 基本 ACL 2000 配置规则 0，并为该规则配置描述信息。

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule 0 permit source 1001::1 128
[Sysname-acl6-basic-2000] rule 0 comment This rule is used on Ethernet 1/1.
```

1.1.22 rule remark

【命令】

rule [*rule-id*] **remark** *text*

undo rule [*rule-id*] **remark** [*text*]

【视图】

WLAN ACL 视图/IPv4 基本 ACL 视图/IPv4 高级 ACL 视图/IPv6 基本 ACL 视图/IPv6 高级 ACL 视图/二层 ACL 视图/用户自定义 ACL 视图

【缺省级别】

2：系统级

【参数】

rule-id：指定规则的编号（该编号对应的规则可以存在也可以不存在），取值范围为 0～65534。该编号用来确定规则注释信息显示的位置：

- 在配置顺序下：若该编号与现有某规则的编号相同，则该注释信息将紧邻该规则之前显示；否则，将按照编号由小到大显示。
- 在自动排序下：若该编号与现有某规则的编号相同，则该注释信息将紧邻该规则之前显示；否则，将在所有规则的最后显示。

text：表示规则注释信息，为 1～63 个字符的字符串，区分大小写。

【描述】

rule remark 命令用来配置规则注释信息。**undo rule remark** 命令用来删除规则注释信息。

缺省情况下，ACL 内没有任何规则注释信息。

需要注意的是：

- 使用 **rule remark** 命令时，如果没有指定 *rule-id* 参数，系统将按照步长从 0 开始，自动分配一个大于现有最大编号的最小编号。
- 使用 **undo rule remark** 命令时，如果没有指定 *rule-id* 和 *text* 参数，将删除所有规则注释信息；如果没有指定 *rule-id* 但指定了 *text* 参数，则只删除指定内容的规则注释信息。
- 用户可以通过 **display this** 和 **display current-configuration** 命令查看配置好的规则注释信息。

相关配置可参考“基础配置命令参考/配置文件管理”中的命令 **display this** 和 **display current-configuration**。

【举例】

在 IPv4 基本 ACL 2000 的视图下显示当前生效的配置信息，查看已有的规则。

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] display this
#
acl number 2000
 rule 0 permit source 14.1.1.0 0.0.0.255
 rule 5 permit source 10.1.1.1 0 time-range work-time
 rule 10 permit source 192.168.0.0 0.0.0.255
```

```
 rule 15 permit source 1.1.1.1 0
 rule 20 permit source 10.1.1.1 0
 rule 25 permit counting
#
return
```

假设规则编号为 10～25 的这四条规则是为 VIP 用户制订的，为方便后续维护，对这四条规则进行如下注释：开头和结尾分别注释为“Rules for VIP_start”和“Rules for VIP_end”。

```
[Sysname-acl-basic-2000] rule 10 remark Rules for VIP_start
[Sysname-acl-basic-2000] rule 26 remark Rules for VIP_end
```

再次在该 ACL 的视图下显示当前生效的配置信息，查看所配置的规则注释信息。

```
[Sysname-acl-basic-2000] display this
#
acl number 2000
 rule 0 permit source 14.1.1.0 0.0.0.255
 rule 5 permit source 10.1.1.1 0 time-range work-time
 rule 10 remark Rules for VIP_start
 rule 10 permit source 192.168.0.0 0.0.0.255
 rule 15 permit source 1.1.1.1 0
 rule 20 permit source 10.1.1.1 0
 rule 25 permit counting
 rule 26 remark Rules for VIP_end
#
return
```

由此可见，在规则编号为 10～25 的这四条规则的前、后均已插入了相应的注释信息。

1.1.23 step

【命令】

step *step-value*

undo step

【视图】

WLAN ACL 视图/IPv4 基本 ACL 视图/IPv4 高级 ACL 视图/IPv6 基本 ACL 视图/IPv6 高级 ACL 视图/二层 ACL 视图

MSR 系列路由器各款型对于本节所描述的命令及参数的支持情况有所不同，详细差异信息如下：

型号	命令	描述
MSR 900	WLAN ACL视图	支持
MSR 930		不支持
MSR 20-1X		支持
MSR 20		支持
MSR 30		支持
MSR 50		支持（MPU-G2不支持）
MSR 2600		支持

【缺省级别】

2：系统级

【参数】

step-value：表示规则编号的步长值，取值范围为 1～20。

【描述】

step 命令用来配置规则编号的步长。**undo step** 命令用来恢复缺省情况。

缺省情况下，规则编号的步长为 5。

相关配置可参考命令 **display acl** 和 **display acl ipv6**。

【举例】

将基本 ACL 2000 的规则编号的步长配置为 2。

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] step 2
```

将 IPv6 基本 ACL 2000 的规则编号的步长配置为 2。

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] step 2
```

1.1.24 time-range

【命令】

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* }

undo 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*]

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

time-range-name：指定时间段的名称，为 1～32 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，时间段的名称不允许使用英文单词 all。

start-time **to** *end-time*：指定周期时间段的时间范围。*start-time* 表示起始时间，格式为 hh:mm，取值范围为 00:00～23:59；*end-time* 表示结束时间，格式为 hh:mm，取值范围为 00:00～24:00，且结束时间必须大于起始时间。

days：指定周期时间段在每周的周几生效。本参数可输入多次，但后输入的值不能与此前输入的值完全重叠（譬如输入 **6** 后不允许再输入 **sat**，但允许再输入 **off-day**），系统将取各次输入值的并集

作为最终值（譬如依次输入 **1**、**wed** 和 **working-day** 之后，最终生效的时间将为每周的工作日）。本参数可输入的形式如下：

- 数字：取值范围为 0～6，依次表示周日～周六；
- 周几的英文缩写（从周日到周六依次为 **sun**、**mon**、**tue**、**wed**、**thu**、**fri** 和 **sat**）；
- 工作日（**working-day**）：表示从周一到周五；
- 休息日（**off-day**）：表示周六和周日；
- 每日（**daily**）：表示一周七天。

from *time1 date1*：指定绝对时间段的起始时间。*time1* 的格式为 hh:mm，取值范围为 00:00～23:59。*date1* 的格式为 MM/DD/YYYY 或 YYYY/MM/DD。MM 表示月，取值范围为 1～12；DD 表示日，取值范围取决于所输入的月份；YYYY 表示年，取值范围为 1970～2100。若未指定本参数，绝对时间段的起始时间将为系统可表示的最早时间，即 1970 年 1 月 1 日 0 点 0 分。

to *time2 date2*：指定绝对时间段的结束时间。*time2* 的格式为 hh:mm，取值范围为 00:00～24:00。*date2* 的格式为 MM/DD/YYYY 或 YYYY/MM/DD。MM 表示月，取值范围为 1～12；DD 表示日，取值范围取决于所输入的月份；YYYY 表示年，取值范围为 1970～2100。结束时间必须大于起始时间。若未指定本参数，绝对时间段的结束时间将为系统可表示的最晚时间，即 2100 年 12 月 31 日 24 点 0 分。

【描述】

time-range 命令用来创建一个时间段，来描述一个特定的时间范围。**undo time-range** 命令用来删除一个时间段。

缺省情况下，不存在任何时间段。

需要注意的是：

- 使用 **time-range** 命令时，如果指定名称的时间段不存在，则创建一个新的时间段（最多 256 个）；如果指定名称的时间段已存在，则对旧时间段进行修改，即在其原有内容的基础上叠加新的内容。
- 使用 *start-time* **to** *end-time days* 这组参数所创建的时间段为周期时间段，它将以一周为周期循环生效；使用 **from** *time1 date1* 和 **to** *time2 date2* 这组参数所创建的时间段为绝对时间段，它将在指定时间范围内生效；而同时使用了上述两组参数所创建的时间段，将取周期时间段和绝对时间段的交集作为生效的时间范围，譬如：创建一个时间段，既定义其在每周一的 8 点到 12 点生效，又定义其在 2010 年全年生效，那么其最终将在 2010 年全年内每周一的 8 点到 12 点生效。
- 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。

相关配置可参考命令 **display time-range**。

【举例】

创建名为 t1 的时间段，其时间范围为每周工作日的 8 点到 18 点。

```
<Sysname> system-view
[Sysname] time-range t1 8:0 to 18:0 working-day
```

创建名为 t2 的时间段，其时间范围为 2010 年全年。

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

```
[Sysname] time-range t2 from 0:0 1/1/2010 to 24:0 12/31/2010
```

创建名为 t3 的时间段，其时间范围为 2010 年全年内每周休息日的 8 点到 12 点。

```
<Sysname> system-view
[Sysname] time-range t3 8:0 to 12:0 off-day from 0:0 1/1/2010 to 24:0 12/31/2010
```

创建名为 t4 的时间段，其时间范围为 2010 年 1 月和 6 月内每周一的 10 点到 12 点以及每周三的 14 到 16 点。

```
<Sysname> system-view
[Sysname] time-range t4 10:0 to 12:0 1 from 0:0 1/1/2010 to 24:0 1/31/2010
[Sysname] time-range t4 14:0 to 16:0 3 from 0:0 6/1/2010 to 24:0 6/30/2010
```

目 录

1 QoS策略

1.1 定义类的命令

1.1.1 display traffic classifier

【命令】

display traffic classifier { **system-defined** | **user-defined** } [*classifier-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

system-defined：系统预定义类。

user-defined：用户定义类。

classifier-name：类名，为 1～31 个字符的字符串。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display traffic classifier 命令用来显示配置的类信息。

如果未指定类名，本命令将显示所有系统预定义类或所有用户定义类的信息。

【举例】

显示配置的用户自定义的类信息。

```
<Sysname> display traffic classifier user-defined
User Defined Classifier Information:
 Classifier: USER1
  Operator: AND
  Rule(s) : If-match ip-precedence 5

 Classifier: database
  Operator: AND
  Rule(s) : If-match acl 3131
            If-match inbound-interface Ethernet1/1
```

表1-1 display traffic classifier user-defined 命令显示信息描述表

字段	描述
User Defined Classifier Information	用户自定义类的信息
Classifier	类的名字及其内容，内容可以有多种类型
Operator	分类规则之间的逻辑关系
Rule	分类规则

1.1.2 if-match

【命令】

if-match [**not**] *match-criteria*

undo if-match [**not**] *match-criteria*

undo if-match [**not**] **acl** [**ipv6**] { *acl-number* | **name** *acl-name* } [**update acl** [**ipv6**] { *acl-number* | **name** *acl-name* }]

【视图】

类视图

【缺省级别】

2：系统级

【参数】

not：不匹配该规则。

match-criteria：类的匹配规则，具体情况如 表 1-2 所示。

acl [**ipv6**] { *acl-number* | **name** *acl-name* }：指定匹配 ACL 的规则。

update acl [**ipv6**] { *acl-number* | **name** *acl-name* }：更改流分类规则中引用的 ACL，将源 ACL 变更为新的 ACL。

表1-2 类的匹配规则取值

取值	描述
acl [**ipv6**] { *acl-number* | **name** *acl-name* }	定义匹配ACL的规则 *acl-number*是ACL的序号，IPv4 ACL序号的取值范围是2000～5999，IPv6 ACL序号的取值范围是2000～3999 *acl-name*是ACL的名称，为1～63个字符的字符串，不区分大小写，必须以英文字母a～z或A～Z开头，为避免混淆，ACL的名称不可以使用英文单词all
any	定义匹配所有数据包的规则
classifier *classifier-name*	定义匹配QoS类的规则，*classifier-name*为类名
customer-dot1p *8021p-list*	定义匹配用户网络802.1p优先级的规则，*8021p-list*为802.1p优先级值的列表，最多可以输入8个802.1p优先级值，802.1p优先级取值范围为0～7
customer-vlan-id { *vlan-id-list* | *vlan-id1* **to** *vlan-id2* }	定义匹配用户网络VLAN ID的规则，*vlan-id-list*为VLAN ID的列表，最多可以输入8个VLAN ID，*vlan-id1* **to** *vlan-id2*表示一个VLAN ID的范围，*vlan-id1*的值必

取值	描述
	须小于*vlan-id2*的值，VLAN ID取值范围为1～4094
destination-mac *mac-address*	定义匹配目的MAC地址的规则
dscp *dscp-list*	定义匹配DSCP的规则，*dscp-list*为DSCP取值的列表，最多可以输入8个DSCP取值，DSCP取值范围为0～63
fr-de	定义匹配FR报文的DE标志
inbound-interface *interface-type interface-number*	定义匹配入接口的规则，*interface-type interface-number*为接口类型和接口编号
ip-precedence *ip-precedence-list*	定义匹配IP优先级的规则，*ip-precedence-list*为ip-precedence的列表，最多可以输入8个ip-precedence，ip-precedence取值范围为0～7
mpls-exp *exp-list*	定义匹配MPLS EXP优先级的规则，*exp-list*为EXP的列表，最多可以输入8个EXP，EXP取值范围为0～7
protocol *protocol-name*	定义匹配协议的规则
protocol-group *protocol-group-id*	定义匹配协议规则组号的规则，*protocol-group-id*为协议规则组号，取值范围为1～64
qos-local-id *local-id-value*	定义匹配qos-local-id的规则，*local-id-value*为QoS本地ID，取值范围为1～4095
rtp start-port *start-port-number* **end-port** *end-port-number*	定义匹配RTP协议端口的规则。*start-port-number*为起始RTP端口号，取值范围为2000～65535；*end-port-number*为结束RTP端口号，取值范围为2000～65535
source-mac *mac-address*	定义匹配源MAC地址的规则

【描述】

if-match 命令用来定义匹配指定匹配规则的所有报文的规则。**undo if-match** 命令用来删除匹配指定匹配规则的所有报文的规则。

if-match not 命令用来定义不匹配指定匹配规则的所有报文的规则。**undo if-match not** 命令用来删除不匹配指定匹配规则的所有报文的规则。

在定义各个规则的时候，注意事项如下：

(1) 定义匹配 ACL 的规则

- 如果类中引用的 ACL 不存在，则不能在硬件中下发。
- 对同一个类，允许通过 ACL 名称和序号的方式分别引用一次同一个 ACL。

(2) 定义匹配目的 MAC 地址规则

- 一个类下可配置多条这样的命令，各个配置之间互相不覆盖。
- 匹配目的 MAC 地址规则只对以太网类型的接口有意义。

(3) 定义匹配源 MAC 地址规则

- 一个类下可配置多条这样的命令，各个配置之间互相不覆盖。
- 匹配源 MAC 地址规则只对以太网类型的接口有意义。

(4) 定义匹配类的规则

如果匹配类的规则之间既有逻辑与，又有逻辑或的关系，采用本匹配方法可以解决。

例如，需要定义 classA，满足以下关系：规则 1 & 规则 2 | 规则 3，可以这样定义：

- traffic classifier classB operator and
- if-match 规则 1
- if-match 规则 2
- traffic classifier classA operator or
- if-match 规则 3
- if-match classifier classB

一个类下可配置多条这样的命令，各个配置之间互相不覆盖。

(5) 定义匹配 DSCP 的规则

- 一个类下可配置多条这样的命令，各个配置之间互相不覆盖。每条命令在配置后，*dscp* 值将自动按照从小到大的顺序排序。
- 一条命令可以配置多个 DSCP 值，最多可指定 8 个；如果指定了多个相同的 DSCP 值，系统默认为一个；多个不同的 DSCP 值是或的关系，即只要有一个值匹配，就算匹配这条规则。
- 删除某条匹配 DSCP 的规则时，指定的所有 DSCP 值必须与该规则中定义的完全相同才会删除，顺序可不一样。

(6) 定义匹配用户网络的 802.1p 优先级的规则

- 一个类下可配置多条这样的命令，各个配置之间互相不覆盖。每条命令在配置后，*8021p* 值将自动按照从小到大的顺序排序。
- 一条命令可以配置多个 802.1p 优先级值，最多可指定 8 个；如果指定了多个相同的 802.1p 优先级值，系统默认为一个；多个不同的 802.1p 优先级值是或的关系，即只要有一个值匹配，就算匹配这条规则。
- 删除某条匹配 802.1p 优先级的规则时，指定的所有 802.1p 优先级值必须与该规则中定义的完全相同才会删除，顺序可不一样。

(7) 定义匹配 FR 报文的 DE 标志规则

一个类下只可配置一条这样的命令。

(8) 定义匹配入接口的规则

- 一个类下可配置多条这样的命令，各个配置之间互相不覆盖。
- 定义该匹配规则时，指定接口必须存在。如果接口为动态接口，在该接口删除后，该规则被删除。
- 支持接口类型：ATM、以太网接口、串口、Tunnel、VT 等。

(9) 定义匹配 IP 优先级的规则

- 一个类下可配置多条这样的命令，各个配置之间互相不覆盖。每条命令在配置后，IP 优先级的值将自动按照从小到大的顺序排序。
- 一条命令可以配置多个 IP 优先级值，最多可指定 8 个；如果指定了多个相同的 IP 优先级值，系统默认为一个；多个不同的 IP 优先级值是或的关系，即只要有一个值匹配，就算匹配这条规则。
- 删除某条匹配 IP 优先级的规则时，指定的所有 IP 优先级值必须与该规则中定义的完全相同才会删除，顺序可不一样。

(10) 定义匹配本地优先级的规则

- 一个类下可配置多条这样的命令，各个配置之间互相不覆盖。每条命令在配置后，本地优先级的值将自动按照从小到大的顺序排序。
- 一条命令可以配置多个本地优先级值，最多可指定 8 个；如果指定了多个相同的本地优先级值，系统默认为一个；多个不同的本地优先级值是或的关系，即只要有一个值匹配，就算匹配这条规则。
- 删除某条匹配本地优先级的规则时，指定的所有本地优先级值必须与该规则中定义的完全相同才会删除，顺序可不一样。

(11) 定义匹配 MPLS EXP 优先级的规则

- 一个类下可配置多条这样的命令，各个配置之间互相不覆盖。每条命令在配置后，MPLS EXP 优先级的值将自动按照从小到大的顺序排序。
- 一条命令可以配置多个 MPLS EXP 优先级值，最多可指定 8 个；如果指定了多个相同的 MPLS EXP 优先级值，系统默认为一个；多个不同的 MPLS EXP 优先级值是或的关系，即只要有一个值匹配，就算匹配这条规则。
- 删除某条匹配 MPLS EXP 优先级的规则时，指定的所有 MPLS EXP 优先级值必须与该规则中定义的完全相同才会删除，顺序可不一样。
- MPLS EXP 为 MPLS 报文特有的参数，该匹配规则仅对 MPLS 报文生效。
- 对于软转发 QoS，MPLS 报文不支持匹配 IP 相关匹配规则。

(12) 定义匹配 RTP 协议端口的规则

- 该命令用于匹配落在指定 RTP 端口号范围内的 RTP 报文，即匹配所有在 *start-port-number* 与 *end-port-number* 之间的偶数 UDP 端口号的报文。
- 一个类下如果多次重复使用该命令，最后一次配置生效。

(13) 定义匹配用户网络 VLAN ID 的规则

- 一个类下可配置多条这样的命令，各个配置之间互相不覆盖。每条命令在配置后，*vlan-id* 值将自动按照从小到大的顺序排序。
- 一条命令可以配置多个 VLAN ID 值，如果指定了多个相同的 VLAN ID 值，系统默认为一个；多个不同的 VLAN ID 值是或的关系，即只要有一个值匹配，就算匹配这条规则。
- 删除某条匹配 VLAN ID 的规则时，指定的所有 VLAN ID 值必须与该规则中定义的完全相同才会删除，顺序可不一样。

相关配置可参考命令 **traffic classifier**。

【举例】

定义类匹配协议不是 IP 的报文。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match not protocol ip
```

定义类 class1 的匹配规则为：匹配目的 MAC 地址为 0050-ba27-bed3 的报文。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match destination-mac 0050-ba27-bed3
```

定义类 class2 的匹配规则为：匹配源 MAC 地址为 0050-ba27-bed2 的报文。

```
<Sysname> system-view
[Sysname] traffic classifier class2
```

```
[Sysname-classifier-class2] if-match source-mac 0050-ba27-bed2
```

定义类 class1 的匹配规则为：匹配用户网络 802.1p 优先级为 3。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match customer-dot1p 3
```

定义类匹配 ACL3101。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl 3101
```

定义类匹配 ACL flow。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl name flow
```

定义类匹配 IPv6 ACL3101。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl ipv6 3101
```

定义类匹配 IPv6 ACL flow。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl ipv6 name flow
```

定义匹配所有数据包的规则。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match any
```

#定义 class1 的匹配规则为：匹配 IP 优先级为 5。定义类 class2，匹配规则为匹配 class1，并且目的 MAC 地址为 0050-BA27-BED3 的报文。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match ip-precedence 5
[Sysname-classifier-class1] quit
[Sysname] traffic classifier class2
[Sysname-classifier-class2] if-match classifier class1
[Sysname-classifier-class2] if-match destination-mac 0050-BA27-BED3
```

定义类 class1 的匹配规则为：匹配 DSCP 值为 1 或 6 或 9 的报文。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match dscp 1 6 9
```

定义类 class1 的匹配规则为：匹配带有 DE 标志的 FR 报文。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match fr-de
```

定义类匹配从 Ethernet1/1 进入的报文。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match inbound-interface ethernet1/1
```

定义类 class1 的匹配规则为：匹配 IP 优先级值为 1 或 6 的报文。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match ip-precedence 1 6
```

定义类匹配 IP 协议的报文。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match protocol ip
```

定义类 class1 的匹配规则为：匹配 RTP 端口号在 16384 和 32767 之间的偶数 UDP 端口号的报文。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match rtp start-port 16384 end-port 32767
```

定义类 class1 的匹配规则为：匹配用户网络 VLAN ID 值为 1 或 6 或 9 的报文。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match customer-vlan-id 1 6 9
```

定义类匹配 qos-local-id 3。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match qos-local-id 3
```

将类 class1 的匹配规则从 ACL 2008 更新为 ACL 2009。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl 2008
[Sysname-classifier-class1] undo if-match acl 2008 update acl 2009
```

定义类 class1 匹配协议规则组 2。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match protocol-group 2
```

1.1.3 traffic classifier

【命令】

traffic classifier *classifier-name* [**operator** { **and** | **or** }]

undo traffic classifier *classifier-name*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

classifier-name：类名，为 1～31 个字符的字符串。

operator：指定各规则之间的逻辑运算符。

and：指定类下的规则之间是逻辑与的关系，即数据包必须匹配全部规则才属于该类。

or：指定类下的规则之间是逻辑或的关系，即数据包只要匹配其中任何一个规则就属于该类。

【描述】

traffic classifier 命令用来定义一个类并进入类视图。**undo traffic classifier** 命令用来删除一个类。

缺省情况下为 **operator and**。

类名 *classifier-name* 不允许为系统预定义类。系统预定义的类如下：

default-class、ef、af1、af2、af3、af4、ip-prec0、ip-prec1、ip-prec2、ip-prec3、ip-prec4、ip-prec5、ip-prec6、ip-prec7、mpls-exp0、mpls-exp1、mpls-exp2、mpls-exp3、mpls-exp4、mpls-exp5、mpls-exp6、mpls-exp7。

相关配置可参考命令 **qos policy**、**qos apply policy** 和 **classifier behavior**。

【举例】

定义一个名为 class1 的类。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1]
```

1.1 定义流行为的命令

1.1.1 car

【命令】

car cir { *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**pir** *peak-information-rate*] | **percent** *percentage* [**cbs** *committed-burst-size-ms* [**ebs** *excess-burst-size-ms*]] } [**green** *action*] [**red** *action*]

undo car

【视图】

流行为视图

【缺省级别】

2：系统级

【参数】

cir *committed-information-rate*：承诺信息速率。流量的平均速率，单位为 kbps。

cbs *committed-burst-size*：承诺突发尺寸，缺省取值为 500 毫秒以 CIR 速率通过的流量，单位为 byte。

ebs *excess-burst-size*：超出突发尺寸，缺省值为 0，单位为 byte。

percent *percentage*：以占用接口带宽的百分比的形式对 **cir** 进行配置，取值范围为 1～100。

cbs *committed-burst-size-ms*：**cir** 以百分比方式配置时的承诺突发尺寸，取值范围为 50～2000，缺省值为 500，单位为毫秒。

ebs *excess-burst-size-ms*：**cir** 以百分比方式配置时的超出突发尺寸，取值范围为 0～2000，缺省取值为 0，单位为毫秒。

green *action*：数据包的流量符合承诺速率时对数据包采取的动作，缺省动作为 **pass**。

red *action*：数据包的流量既不符合承诺速率也不符合峰值速率时对数据包采取的动作，缺省动作为 **discard**。

action：对数据包采取的动作，有以下几种：

- **discard**：丢弃数据包。
- **pass**：允许数据包通过。
- **remark-dscp-pass** *new-dscp*：设置报文新的 DSCP 值，并允许数据包通过，取值范围为 0～63。
- **remark-prec-pass** *new-precedence*：设置新的 IP 优先级，并允许数据包通过，取值范围为 0～7。

【描述】

car 命令用来为流行为配置流量监管动作。**undo car** 命令用来取消流量监管动作配置。

接口或 PVC 上应用的策略中使用 **car** 时，可以应用到接口报文的接收或者发送方向。

需要注意的是：

- 如果接口或 PVC 上既应用了流行为视图下 **car** 命令配置的策略，又配置了 **qos car** 命令，那么只有前者会生效。
- 如果多次使用该命令在同一个流行为上配置，最后一次配置生效。

相关配置可参考命令 **qos policy**、**traffic behavior** 和 **classifier behavior**。

【举例】

为流行为配置流量监管。报文正常流速为 200kbps，承诺突发尺寸为 50000bytes，速率大于 200kbps 时，报文 IP 优先级改为 0 并发送。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] car cir 200 cbs 50000 ebs 0 green pass red remark-prec-pass 0
```

配置 QoS 策略，在流行为中配置 CAR，cir 为接口带宽的 50%，并将在接口上应用该策略。

```
<Sysname> system-view
[Sysname] traffic classifier c1
[Sysname-classifier-c1] if-match any
[Sysname-classifier-c1] quit
[Sysname] traffic behavior b1
[Sysname-behavior-b1] car cir percent 50
[Sysname-behavior-b1] quit
[Sysname] qos policy p1
[Sysname-qospolicy-p1] classifier c1 behavior b1
[Sysname-qospolicy-p1] quit
[Sysname] interface GigabitEthernet 0/1
[Sysname-GigabitEthernet0/1] qos apply policy p1 outbound
```

1.1.2 display traffic behavior

【命令】

display traffic behavior { **system-defined** | **user-defined** } [*behavior-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

system-defined：系统预定义行为。

user-defined：用户定义行为。

behavior-name：行为名，为 1～31 个字符的字符串。如果未指定行为名，则显示所有系统预定义行为或所有用户定义行为的信息。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display traffic behavior 命令用来显示配置的流行为信息。

【举例】

显示配置的用户自定义的流行为信息。

```
<Sysname> display traffic behavior user-defined
User Defined Behavior Information:
  Behavior: test
    Assured Forwarding:
      Bandwidth 30 (Kbps)
      Discard Method: Tail
    General Traffic Shape:
      CIR 300 (kbps), CBS 15000 (byte), EBS 0 (byte),
      Queue length 50 (Packets)
    Marking:
      Remark MPLS EXP 3
    Filter enable: permit
  Behavior: USER1
    Marking:
      Remark IP Precedence 3
    Committed Access Rate:
      CIR 200 (kbps), CBS 15000 (byte), EBS 0 (byte)
```

```
    Green Action: pass
    Red Action: discard
  Expedited Forwarding:
    Bandwidth 50 (Kbps) CBS 1500 (Bytes)
  Nesting:
    Nest Top-Most Vlan-ID  1000
Behavior: USER2
    Mirror enable:
      Mirror type: interface
      Mirror destination: Ethernet0/5
  Redirect enable:
    Redirect type: cpu
    Redirect destination: cpu
  Nest Policy:
    Traffic-policy test
Behavior: USER3
  Flow based Weighted Fair Queue:
    Max number of hashed queues: 1000
    Discard Method: Tail
   Filter enable: deny
```

表1-3 display traffic behavior user-defined 命令显示信息描述表

字段	描述
User Defined Behavior Information	用户自定义流行为的信息
Behavior	行为的名字及其内容，内容可以有多种类型
Assured Forwarding	确保转发（AF队列）的相关信息
Bandwidth	队列的带宽
Discard Method	超出队列带宽时的丢弃方式。共支持尾丢弃Tail、基于IP优先级的随机早期丢弃IP Precedence based WRED和基于DSCP的随机早期丢弃DSCP based WRED三种方式
General Traffic Shape	流量整形（GTS）的相关配置信息
Queue length	队列长度
Marking	重标记的相关信息
Remark	重标记的类型。可支持的类型有DSCP、IP precedence、MPLS EXP、FR DE、dot1p COS、ATM CLP、qos local ID等类型
Filter enable	流量过滤相关信息。过滤功能可以配置允许（permit）和阻止（deny）两种方式
Committed Access Rate	流量限速的相关信息
Green Action	对绿色报文的处理，具体请参考1.1.1 car
Red Action	对红色报文的处理，具体请参考1.1.1 car
Expedited Forwarding	加速转发相关信息
Nesting	插入报文VLAN tag相关配置信息

字段	描述
Mirror enable	流量镜像相关信息
Mirror type	流镜像类型，目前仅支持镜像到interface
Mirror destination	流镜像的目的，对应于interface的是接口名
Redirect enable	流量重定向相关信息
Redirect type	重定向类型，目前支持CPU、interface
Redirect destination	重定向的目的，对应于interface的是接口名
Nest Policy	嵌套policy相关配置信息
Traffic-policy	嵌套的policy名称
Flow based Weighted Fair Queue	基于流的加权公平队列相关信息
Max number of hashed queues	加权公平队列的长度
Filter enable	Netstream相关配置信息。过滤功能可以配置允许（permit）和阻止（deny）两种方式

1.1.3 filter

【命令】

filter { **deny** | **permit** }

undo filter

【视图】

流行为视图

【缺省级别】

2：系统级

【参数】

deny：丢弃数据包。

permit：允许数据包通过。

【描述】

filter 命令用来为流行为配置流量过滤动作。**undo filter** 命令用来取消过滤动作配置。

【举例】

为流行为配置丢弃数据包的过滤动作。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] filter deny
```

1.1.4 gts

【命令】

gts cir *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size* [**queue-length** *queue-length*]]]

undo gts

【视图】

流行为视图

【缺省级别】

2：系统级

【参数】

cir *committed-information-rate*：承诺信息速率，单位为 kbps。

cbs *committed-burst-size*：承诺突发尺寸，实际平均速率在承诺速率以内时的突发流量，单位为 byte。

ebs *excess-burst-size*：超出突发尺寸，单位为 byte，缺省值为 0。

queue-length *queue-length*：队列的最大长度，缺省值为 50。

【描述】

gts 命令用来采用绝对值的方式为流行为配置流量整形动作。**undo gts** 命令用来取消流量整形动作配置。

接口或 PVC 上应用的策略中使用 **gts** 时，只能应用到接口的出方向。

接口或 PVC 上应用配置了 **gts** 的策略将导致原有的 **qos gts** 命令失效。

如果多次使用该命令在同一个流行为上配置，最后一次的配置将覆盖前面的配置。

相关配置可参考命令 **gts percent**、**qos policy**、**traffic behavior** 和 **classifier behavior**。

【举例】

为流行为配置 GTS，正常流速为 200kbps，承诺突发尺寸为 50000bytes，速率大于 200kbps 时，将进入队列缓存，缓存队列长度为 100。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] gts cir 200 cbs 50000 ebs 0 queue-length 100
```

1.1.5 gts percent

【命令】

gts percent cir *cir-percent* [**cbs** *cbs-time* [**ebs** *ebs-time*]]

undo gts

【视图】

流行为视图

【缺省级别】

2：系统级

【参数】

cir *cir-percent*：承诺信息速率百分比，取值范围为 0～100。CIR 的实际值是百分比值乘以接口带宽值。

cbs *cbs-time*：某段时间内的承诺突发尺寸，单位为 ms，缺省值为 500ms。CBS 的实际值是 CBS 的配置时间值乘以 CIR 的实际值。

ebs *ebs-time*：某段时间内的超出突发尺寸，单位为 ms，缺省值为 0ms。EBS 的实际值是 EBS 的配置时间值乘以 CIR 的实际值。

【描述】

gts percent 命令用来采用百分比的方式为流行为配置流量整形动作。**undo gts** 命令用来取消流量整形动作配置。

接口或 PVC 上应用的策略中使用 **gts** 时，只能应用到接口的出方向。

接口或 PVC 上应用配置了 **gts** 的策略将导致原有的 **qos gts** 命令失效。

如果多次使用该命令在同一个流行为上配置，最后一次的配置将覆盖前面的配置。

相关配置可参考命令 **gts**、**qos policy**、**traffic behavior** 和 **classifier behavior**。

【举例】

配置使用流量整形，正常流量为 50%的接口带宽，在第一时间可以有 200ms×50%接口带宽的突发流量通过，以后速率小于等于 50%的接口带宽时正常发送，速率大于 50%的接口带宽时，将进入队列缓存。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] gts percent cir 50 cbs 200
```

1.1.6 redirect

【命令】

redirect { **cpu** | **interface** *interface-type interface-number* }

undo redirect { **cpu** | **interface** *interface-type interface-number* }

【视图】

流行为视图

【缺省级别】

2：系统级

【参数】

cpu：重定向到 CPU。

interface：重定向到指定的接口。

interface-type interface-number：指定接口类型和接口编号。

【描述】

redirect 命令用来为流行为配置流量重定向动作。**undo redirect** 命令用来取消流量重定向动作配置。

MSR 系列路由器各款型对于本节所描述的命令及参数的支持情况有所不同，详细差异信息如下：

型号	命令	参数	描述
MSR 900	**redirect**	**cpu**、**interface**	不支持
MSR 930			不支持
MSR 20-1X			不支持
MSR 20			仅支持**cpu**
MSR 30			30-11E、30-11F支持 MIM二层以太网交换模块支持
MSR 50			FIC二层以太网交换模块支持
MSR 2600			支持

【举例】

为流行为配置流量重定向动作，重定向到 Ethernet1/1。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] redirect interface ethernet1/1
```

1.1.7 remark dot1p

【命令】

remark dot1p *8021p*

undo remark dot1p

【视图】

流行为视图

【缺省级别】

2：系统级

【参数】

8021p：标记的 802.1p 优先级，取值范围为 0～7。

【描述】

remark dot1p 命令用来配置标记报文的 802.1p 优先级。**undo remark dot1p** 命令用来取消配置。

相关配置可参考命令 **qos policy**、**traffic behavior** 和 **classifier behavior**。

【举例】

配置标记报文的 802.1p 优先级值为 2。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark dot1p 2
```

1.1.8 remark dscp

【命令】

remark dscp *dscp-value*

undo remark dscp

【视图】

流行为视图

【缺省级别】

2：系统级

【参数】

dscp-value：DSCP值，取值范围为 0～63，也可以是关键字，如 表 1-4 所示。

表1-4 DSCP 关键字与值的对应表

关键字	DSCP 值（二进制）	DSCP 值（十进制）
default	000000	0
af11	001010	10
af12	001100	12
af13	001110	14
af21	010010	18
af22	010100	20
af23	010110	22
af31	011010	26
af32	011100	28
af33	011110	30
af41	100010	34
af42	100100	36
af43	100110	38
cs1	001000	8
cs2	010000	16
cs3	011000	24
cs4	100000	32
cs5	101000	40
cs6	110000	48
cs7	111000	56
ef	101110	46

【描述】

remark dscp 命令用来为类配置标记报文的 DSCP 值。**undo remark dscp** 命令用来取消标记报文的 DSCP 值。

相关配置可参考命令 **qos policy**、**traffic behavior** 和 **classifier behavior**。

【举例】

配置标记报文的 DSCP 值为 6。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark dscp 6
```

1.1.9 remark ip-precedence

【命令】

remark ip-precedence *ip-precedence-value*

undo remark ip-precedence

【视图】

流行为视图

【缺省级别】

2：系统级

【参数】

ip-precedence-value：标记的 IP 优先级，取值范围为 0～7。

【描述】

remark ip-precedence 命令用来配置标记报文的 IP 优先级。**undo remark ip-precedence** 命令用来取消标记报文的 IP 优先级。

相关配置可参考命令 **qos policy**、**traffic behavior** 和 **classifier behavior**。

【举例】

配置标记报文的 IP 优先级值为 6。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark ip-precedence 6
```

1.1.10 remark qos-local-id

【命令】

remark qos-local-id *local-id-value*

undo remark qos-local-id

【视图】

流行为视图

【缺省级别】

2：系统级

【参数】

local-id-value：标记的 QoS 本地 ID 值，取值范围为 1～4095。

【描述】

remark qos-local-id 命令用来配置标记报文的 qos-local-id 值。**undo remark qos-local-id** 命令用来取消标记报文的 qos-local-id 值。

【举例】

配置标记报文的 qos-local-id 值为 2。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark qos-local-id 2
```

1.1.11 traffic behavior

【命令】

traffic behavior *behavior-name*

undo traffic behavior *behavior-name*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

behavior-name：流行为名，为 1～31 个字符的字符串。

【描述】

traffic behavior 命令用来定义一个流行为并进入流行为视图。**undo traffic behavior** 命令用来删除一个流行为。

行为名 *behavior–name* 不能和系统预定义的流行为名相同。系统预定义的流行为有 ef、af、be、be-flow-based 等。

相关配置可参考命令 **qos policy**、**qos apply policy** 和 **classifier behavior**。

【举例】

定义一个名为 behavior1 的流行为。

```
<Sysname> system-view
[Sysname] traffic behavior behavior1
[Sysname-behavior-behavior1]
```

1.1.12 traffic-policy

【命令】

traffic-policy *policy-name*

undo traffic-policy

【视图】

流行为视图

【缺省级别】

2：系统级

【参数】

policy-name：策略名，为 1～31 个字符的字符串。必须是已经存在的策略。

【描述】

traffic-policy 命令用来在父策略流行为视图下应用一个子策略。**undo traffic-policy** 命令用来删除关联的子策略。

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。

需要注意的是：

- 在父策略行为下应用子策略时，最多只能嵌套一层策略，并且不能嵌套自己。
- 一个流行为中至多只能嵌套一个子策略。
- 如果父策略和子策略中配置了相同的行为，先执行父策略的行为再执行子策略的行为。
- 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 带宽配置不允许采用绝对值形式。
- 子策略中不允许配置 GTS。
- 嵌套策略支持对 IPv4、IPv6、MPLS 报文的处理。
- 如果嵌套策略已经应用在接口或 PVC 上，则不允许删除嵌套的子策略，必须先解除子策略和父策略的嵌套关系。

相关配置可参考命令 **traffic behavior** 和 **traffic classifier**。

【举例】

配置策略嵌套，在父策略下应用子策略 child。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] traffic-policy child
```

1.2 定义策略和应用策略的命令

1.2.1 classifier behavior

【命令】

classifier *classifier-name* **behavior** *behavior-name*

undo classifier *classifier-name*

【视图】

策略视图

【缺省级别】

2：系统级

【参数】

classifier-name：类名，为 1～31 个字符的字符串。

behavior-name：流行为名，为 1～31 个字符的字符串。

【描述】

classifier behavior 命令用来在策略中为类指定采用的流行为。**undo classifier** 命令用来取消指定类在策略中的使用。

需要注意的是：

- 策略下每个类只能与一个动作关联。
- 如果配置本命令时指定的类和流行为不存在，系统将创建一个空的类和空的流行为。
- 对缺省类不能使用 **undo** 命令。

相关配置可参考命令 **qos policy**，“三层技术-IP 路由命令参考/路由策略”中的命令 **route-policy**。

【举例】

在策略 user1 中为类 database 指定采用流行为 test。

```
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1] classifier database behavior test
[Sysname-qospolicy-user1]
```

1.2.2 display qos policy

【命令】

display qos policy { **system-defined** | **user-defined** } [*policy-name* [**classifier** *classifier-name*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

system-defined：系统预定义策略。

user-defined：用户定义策略。

policy-name：策略名，为 1～31 个字符的字符串。如果未指定，则显示所有系统预定义策略或所有用户定义策略的配置信息。

classifier-name：策略中的类名。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display qos policy 命令用来显示系统预定义策略或用户定义策略的配置信息。

【举例】

显示用户定义策略的配置信息。

```
<Sysname> display qos policy user-defined
  User Defined QoS Policy Information:
  Policy: test
   Classifier: default-class
     Behavior: be
      -none-
   Classifier: USER1
     Behavior: USER1
      Marking:
        Remark IP Precedence 3
      Committed Access Rate:
        CIR 200 (kbps), CBS 15000 (byte), EBS 0 (byte)
        Green Action: pass
        Red  Action: discard
      Expedited Forwarding:
        Bandwidth 50 (Kbps) CBS 1500 (Bytes)
   Classifier: database
     Behavior: database
      Assured Forwarding:
        Bandwidth 30 (Kbps)
        Discard Method: Tail
        Queue Length  : 64 (Packets)
      General Traffic Shape:
        CIR 300 (kbps), CBS 15000 (byte), EBS 0 (byte)
        Queue length 50 (Packets)
      Marking:
        Remark MPLS EXP 3
```

表1-5 display qos policy 命令显示信息描述表

字段	描述
Policy	策略名
Classifier	类名，一个策略中可以存在多个类，每个类有对应的行为，每个类的匹配规则又可以有多条，参见**traffic classifier**命令
Behavior	策略中一个类对应的行为，每个行为可以有多条规则，参见**traffic behavior**命令

1.2.3 display qos policy interface

【命令】

display qos policy interface [*interface-type interface-number* [**pvc** { *pvc-name* [*vpi/vci*] | *vpi/vci* }]] [**inbound** | **outbound**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

interface-type interface-number：指定的接口类型和接口编号。

inbound：显示对接口接收到的报文应用的 QoS 策略信息。

outbound：显示对接口发送的报文应用的 QoS 策略信息。

pvc { *pvc-name* [*vpi/vci*] | *vpi/vci* }：只用于 ATM 接口，显示指定 ATM 接口上的指定 PVC 的策略配置。*pvc-name* 表示 PVC 名。*vpi/vci* 表示 VPI/VCI 值。输入本参数时，无法输入参数 **inbound** 或 **outbound**。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display qos policy interface 命令用来显示指定接口、指定 PVC 或所有接口与 PVC 上 QoS 策略的配置信息和运行情况。

如指定接口为 Virtual-Template 接口，将显示继承该 Virtual-Template 接口的所有 Virtual-Access 接口下的 QoS 策略的信息，Virtual-Template 本身无 QoS 信息显示。

【举例】

显示 Ethernet1/1 接口上 QoS 策略的配置信息和运行情况。

```
<Sysname> display qos policy interface ethernet 1/1

  Interface: Ethernet1/1
  Direction: Outbound

  Policy: test
   Classifier: default-class
     Matched : 0(Packets) 0(Bytes)
     5-minute statistics:
```

```
    Forwarded: 0/0 (pps/bps)
    Dropped  : 0/0 (pps/bps)
  Rule(s) : If-match any
  Behavior: be
  Default Queue:
   Flow Based Weighted Fair Queuing
     Max number of hashed queues: 256
     Matched  : 0/0 (Packets/Bytes)
     Enqueued : 0/0 (Packets/Bytes)
     Discarded: 0/0 (Packets/Bytes)
     Discard Method: Tail
Classifier: USER1
  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 5
  Behavior: USER1
   Marking: 0(Packets)
     Remark IP Precedence 3
   Committed Access Rate:
     CIR 200 (kbps), CBS 15000 (byte), EBS 0 (byte)
     Green Action: pass
     Red Action: discard
     Green : 0(Packets) 0(Bytes)
     Red   : 0(Packets) 0(Bytes)
   Expedited Forwarding:
     Bandwidth 50 (Kbps), CBS 1500 (Bytes)
     Matched  : 0/0 (Packets/Bytes)
     Enqueued : 0/0 (Packets/Bytes)
     Discarded: 0/0 (Packets/Bytes)
Classifier: database
  Matched : 0(Packets) 0(Bytes)
  5-minute statistics:
    Forwarded: 0/0 (pps/bps)
    Dropped  : 0/0 (pps/bps)
  Operator: AND
  Rule(s) : If-match acl 3131
            If-match inbound interface Ethernet1/1
  Behavior: database
   General Traffic Shape:
     CIR 300 (kbps), CBS 15000 (byte), EBS 0 (byte)
     Queue Length: 50 (Packets)
     Queue size  : 0 (Packets)
     Passed   : 0(Packets) 0(Bytes)
     Discarded: 0(Packets) 0(Bytes)
     Delayed  : 0(Packets) 0(Bytes)
```

```
  Discard Method: Tail
Marking: 0(Packets)
  Remark MPLS EXP 3
Assured Forwarding:
  Bandwidth 30 (Kbps)
  Matched  : 0/0 (Packets/Bytes)
  Enqueued : 0/0 (Packets/Bytes)
  Discarded: 0/0 (Packets/Bytes)
  Discard Method: Tail
Nest Policy:
  Traffic policy son1
   Classifier: default-class
     Matched : 0/0 (Packets/Bytes)
     5-minute statistics:
       Forwarded: 0/0 (pps/bps)
       Dropped  : 0/0 (pps/bps)
     Rule(s) : If-match any
     Behavior: be
     Default Queue:
      Flow Based Weighted Fair Queuing
        Max number of hashed queues: 256
        Matched  : 0/0 (Packets/Bytes)
        Enqueued : 0/0 (Packets/Bytes)
        Discarded: 0/0 (Packets/Bytes)
        Discard Method: Tail
   Classifier: son1
     Matched : 0/0 (Packets/Bytes)
     5-minute statistics:
       Forwarded: 0/0 (pps/bps)
       Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) : If-match acl 3000
     Behavior: son1
      Marking: 0(Packets)
        Remark MPLS EXP 3
      Committed Access Rate:
        CIR 200 (kbps), CBS 15000 (byte), EBS 0 (byte)
        Green Action: pass
        Red  Action: discard
        Green: 0/0 (Packets/Bytes)
        Red : 0/0 (Packets/Bytes)
      Expedited Forwarding:
        Bandwidth 1000 (Kbps), CBS 25000 (Bytes)
        Matched  : 0/0 (Packets/Bytes)
        Enqueued : 0/0 (Packets/Bytes)
        Discarded: 0/0 (Packets/Bytes)
```

表1-6 display qos policy interface 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号结合在一起组成。
Direction	Policy应用在接口的方向
Policy	应用到接口上的策略的名字
Classifier	策略里分类规则以及对应的配置信息
Matched	符合分类规则的数据包数目
5-minute statistics	最近5分钟的流速统计信息（如果流速统计的策略超过1000个、或者流速统计的分类超过10000个，则统计信息将显示为none）
Forwarded	符合分类规则的成功转发报文在统计周期内的平均速率
Dropped	符合分类规则的丢弃报文在统计周期内的平均速率
Operator	同一个类中多条分类规则的逻辑关系
Rule(s)	类的分类规则
Behavior	策略里行为的名字及配置信息，参见behavior的相关命令
Default Queue	默认队列
Flow Based Weighted Fair Queuing	基于流的加权公平队列
Max number of hashed queues	Hash队列最大数
Matched	队列匹配的包数/字节数
Enqueued	入队包数/字节数
Discarded	丢弃包数/字节数
Discard Method	丢弃方式
Marking	标记相关信息
Remark IP Precedence	重新标记报文的IP优先级值
Remark MPLS EXP	重新标记MPLS报文的EXP值
Committed Access Rate	流量限速的相关信息
CIR	承诺信息速率，单位为kbps
CBS	承诺突发尺寸，也就是容纳突发流量的令牌桶深度，单位为byte
EBS	超出突发尺寸，在双令牌桶算法中超出突发流量超过承诺突发流量的部分，单位为byte
Green Action	对绿色报文的动作
Red Action	对红色报文的动作
Green	绿色报文的流量统计
Red	红色报文的流量统计
Expedited Forwarding	加速转发（EF队列）的相关信息

字段	描述
Assured Forwarding	确保转发（AF队列）的相关信息
Bandwidth	队列可确保的最小带宽
General Traffic Shape	流量整形（GTS）的相关信息
Queue Length	缓冲队列能够容纳的数据包的个数
Queue Size	当前缓冲区中数据包的数目
Passed	已经通过的数据包数目和字节数
Discarded	被丢弃的数据包数目和字节数
Delayed	被延迟发送的数据包数目和字节数
Nest Policy	应用到接口上的策略的子策略
Traffic policy son1	子策略的名称为son1

1.2.4 qos apply policy (interface view, port group view, PVC view)

【命令】

qos apply policy *policy-name* { **inbound** | **outbound** }

undo qos apply policy [*policy-name*] { **inbound** | **outbound** }

【视图】

接口视图/端口组视图/PVC 视图

【缺省级别】

2：系统级

【参数】

inbound：入方向。

outbound：出方向。

policy *policy-name*：策略名，为 1～31 个字符的字符串。

【描述】

qos apply policy 命令用来应用关联的策略。**undo qos apply policy** 命令用来删除关联的策略。

除链路层协议为 X.25、LAPB 协议的接口外，所有物理接口都可以应用 QoS 策略。

在应用策略时，如果策略中为确保转发和加速转发的类指定的带宽之和超过接口或 PVC 允许的可用带宽，则在该接口或 PVC 不可应用。如果对接口或 PVC 修改了可用带宽，此时如果策略中为确保转发和加速转发的类指定的带宽之和超过接口或 PVC 允许的可用带宽，则将策略删除。入方向的策略与类关联的行为不允许有 **queue af**、**queue ef** 与 **queue wfq** 配置，也不允许有 GTS 配置。

在接口视图下执行该命令，则该配置只在当前接口生效；在端口组视图下执行该命令，则该配置将在端口组中的所有端口生效；在 PVC 视图下执行该命令，则该配置只在当前 PVC 生效。

在 VT 接口下执行该命令，则该配置会同步到继承于 VT 接口的所有 VA 接口上去。

在 WLAN-ESS 接口下执行该命令，则该配置会同步到继承于 WLAN-ESS 接口的所有 WLAN-DBSS 接口上去。

策略在接口或 PVC 应用的规则如下：

- 普通物理接口、PVC 和 MP 引用的 VT，可以应用配置了各种特性（包括 remark、car、gts、queue af、queue ef、queue wfq、wred 等）的策略。
- 策略中如果关联了配置了流量整形和队列（queue ef、queue af、queue wfq）特性的行为，则不能作为入方向策略应用在入接口或 PVC 上。

注意

- 对于 VT、Dialer、BRI、PRI 等主通道型接口，如果配置 qos max-bandwidth 命令，af、ef 按照 qos max-bandwidth 的配置值进行队列带宽检测及计算，同步到 VA、B 通道等子通道类型接口上的 af、ef 也按照该值进行检测及计算，忽略子通道接口带宽，此种情况主通道接口及子通道接口 QoS 配置相同，仅输出主通道接口的提示信息；如果未配置 qos max-bandwidth 命令，af、ef 按照 1G Bit 带宽进行计算，同步到子通道的 af、ef 按照 VA、B 通道实际带宽进行队列计算，此种情况下，若子通道接口因带宽变化导致队列失效，将输出子通道接口提示信息。
- 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 CBQ 队列功能生效，同时需要配置 **qos max-bandwidth** 命令以提供 CBQ 计算的基准带宽。

【举例】

将策略 USER1 应用到接口 Ethernet1/1 的出方向上。

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] qos apply policy USER1 outbound
```

1.2.5 qos apply policy (user-profile view)

【命令】

qos apply policy *policy-name* { **inbound** | **outbound** }

undo qos apply policy [*policy-name*] { **inbound** | **outbound** }

【视图】

user-profile 视图

【缺省级别】

2：系统级

【参数】

inbound：入方向，对设备接收的上线用户流量（即上线用户发送的流量）应用策略。

outbound：出方向，对设备发送的上线用户流量（即上线用户接收的流量）应用策略。

policy-name：策略名，为 1～31 个字符的字符串。

【描述】

qos apply policy 命令用来为 User Profile 应用关联的策略。**undo qos apply policy** 命令用来删除关联的策略。

需要注意的是：

- 如果 User Profile 被激活后，不允许修改 User Profile 下的配置，需要禁用后才可以被修改或删除。禁用 User Profile 将导致使用该 User Profile 的用户强制下线。
- 关联的策略只有在 User Profile 处于激活状态、且用户成功上线后才能生效。
- user-profile 视图下应用的策略中的流行为只支持 **remark**、**car**、**filter** 三种动作。
- user-profile 视图下应用的策略不能为空策略。

【举例】

对设备发送的上线用户 user 的流量应用策略 test（该策略已经建立）。

```
<Sysname> system-view
[Sysname] user-profile user
[Sysname-user-profile-user] qos apply policy test outbound
```

1.2.6 qos policy

【命令】

qos policy *policy-name*

undo qos policy *policy-name*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

policy *policy-name*：策略名，为 1～31 个字符的字符串。

【描述】

qos policy 命令用来定义一个策略并进入策略视图。**undo qos policy** 命令用来删除一个策略。

如果该策略已经被应用，则不允许删除该策略，需要先在应用的位置上取消对该策略的应用，然后再使用 **undo qos policy** 命令删除该策略。

策略名 *policy-name* 不允许为系统预定义策略。系统预定义的策略为 default。

相关配置可参考命令 **classifier behavior** 和 **qos apply policy**。

【举例】

定义一个名为 user1 的策略。

```
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1]
```

1.3 接口流速统计配置命令

1.3.1 qos flow-interval

【命令】

qos flow-interval *interval*

undo qos flow-interval

【视图】

接口视图

【缺省级别】

2：系统级

【参数】

interval：流速统计时间，单位为分钟。

【描述】

qos flow-interval 命令用来配置接口流速统计时间。**undo qos flow-interval** 命令用来恢复缺省情况。

缺省情况下，接口流速统计时间为 5 分钟。

流速统计时间及统计结果可通过命令 **display qos policy interface** 查看。

说明

- ATM PVC 的流速统计时间采用所在 ATM 接口的统计时间。
- FR DLCI 的流速统计时间采用所在 FR 接口的统计时间。
- 子接口的流速统计时间采用主接口的统计时间。

【举例】

配置接口 Ethernet1/1 的流速统计时间为 10 分钟。

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] qos flow-interval 10
```

2 优先级映射

2.1 优先级映射表配置命令

2.1.1 display qos map-table

【命令】

display qos map-table [**dot11e-lp** | **dot1p-lp** | **dscp-lp** | **lp-dot11e** | **lp-dot1p**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

dot11e-lp：802.11e 优先级到本地优先级映射表。

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。

lp-dot11e：本地优先级到 802.11e 优先级映射表。

lp-dot1p：本地优先级到 802.1p 优先级映射表。

MSR 系列路由器各款型对于本节所描述的命令及参数的支持情况有所不同，详细差异信息如下：

型号	命令	参数	描述
MSR 900	**display qos map-table**	**dot11e-lp、lp-dot11e、lp-dot1p**	支持
MSR 930			支持
MSR 20-1X			具有WLAN功能的款型支持 安装WLAN模块后支持
MSR 20			安装WLAN模块后支持
MSR 30			安装WLAN模块后支持
MSR 50			安装WLAN模块后支持 MPU-G2、MSR 50-06不支持
MSR 2600			支持

型号	命令	参数	描述
MSR 900	**display qos map-table**	**dscp-lp**	不支持
MSR 930			支持
MSR 20-1X			不支持

型号	命令	参数	描述
MSR 20			不支持
MSR 30			仅30-11E、30-11F支持
MSR 50			不支持
MSR 2600			支持

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display qos map-table 命令用来显示指定优先级映射表配置情况。

如不指定表的类型，本命令将显示所有映射表的配置情况。如不指定方向，本命令将显示所有方向的映射表的配置情况。

相关配置可参考命令 **qos map-table**。

【举例】

显示 802.1p 优先级到本地优先级映射表的配置信息。

```
<Sysname> display qos map-table dot1p-lp
MAP-TABLE NAME: dot1p-lp   TYPE: pre-define
IMPORT  :  EXPORT
   0    :    2
   1    :    0
   2    :    1
   3    :    3
   4    :    4
   5    :    5
   6    :    6
   7    :    7
```

表2-1 display qos map-table 命令显示信息描述表

字段	描述
MAP-TABLE NAME	映射表的名字
TYPE	映射表的类型
IMPORT	映射表的输入值
EXPORT	映射表的输出值

2.1.2 import

【命令】

import *import-value-list* **export** *export-value*

undo import { *import-value-list* | **all** }

【视图】

优先级映射表视图

【缺省级别】

2：系统级

【参数】

import-value-list：映射输入参数列表。

export-value：映射输出参数。

all：删除该映射表所有参数。

【描述】

import 命令用来配置指定优先级映射表参数，定义一条或一组映射规则。**undo import** 命令用来删除指定映射索引所对应的映射项，被删除的映射条目恢复为系统缺省值。

相关配置可参考命令 **display qos map-table**。

【举例】

配置 802.1p 优先级到本地先级映射表参数，与 802.1p 优先级 4、5 相对应的本地优先级为 1。

```
<Sysname> system-view
[Sysname] qos map-table dot1p-lp
[Sysname-maptbl-dot1p-lp] import 4 5 export 1
```

2.1.3 qos map-table

【命令】

qos map-table { **dot11e-lp** | **dot1p-lp** | **dscp-lp** | **lp-dot11e** | **lp-dot1p** }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

dot11e-lp：802.11e 优先级到本地优先级映射表。

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。

lp-dot11e：本地优先级到 802.11e 优先级映射表。

lp-dot1p：本地优先级到 802.1p 优先级映射表。

MSR 系列路由器各款型对于本节所描述的命令及参数的支持情况有所不同，详细差异信息如下：

型号	命令	参数	描述
MSR 900	qos map-table	dot11e-lp、lp-dot11e、lp-dot1p	支持
MSR 930			支持
MSR 20-1X			具有WLAN功能的款型支持 安装WLAN模块后支持
MSR 20			安装WLAN模块后支持
MSR 30			安装WLAN模块后支持
MSR 50			安装WLAN模块后支持 MPU-G2、MSR 50-06不支持
MSR 2600			支持

型号	命令	参数	描述
MSR 900	qos map-table	dscp-lp	不支持
MSR 930			支持
MSR 20-1X			不支持
MSR 20			不支持
MSR 30			仅30-11E、30-11F支持
MSR 50			不支持
MSR 2600			支持

【描述】

qos map-table 命令用来进入指定的优先级映射表视图。

说明

优先级映射表为无方向映射表。

相关配置可参考命令 **display qos map-table**。

【举例】

进入 802.1p 优先级到本地优先级映射表视图。

```
<Sysname> system-view
[Sysname] qos map-table dot1p-lp
[Sysname-maptbl-in-dot1p-lp]
```

2.2 端口优先级配置命令

2.2.1 qos priority

【命令】

qos priority *priority-value*

undo qos priority

【视图】

接口视图/端口组视图

【缺省级别】

2：系统级

【参数】

priority-value：端口优先级值。取值范围为 0～7，缺省值为 0。

【描述】

qos priority 命令用来配置当前端口的端口优先级。**undo qos priority** 命令用来恢复端口优先级为缺省值。

端口优先级可以通过命令 **display qos trust interface** 来查看。

端口优先级的缺省值为 0

【举例】

配置以太网端口 Ethernet1/1 的端口优先级为 2（支持一种类型端口优先级的设备）。

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] qos priority 2
```

2.3 端口优先级信任模式配置命令

2.3.1 display qos trust interface

【命令】

display qos trust interface [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

interface-type interface-number：指定的接口类型和接口编号。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display qos trust interface 命令用来显示当前配置的端口优先级信任模式信息和端口优先级的信息。

如果不指定接口，本命令将显示所有接口的端口优先级信任模式信息。

【举例】

显示当前配置的端口优先级信任模式信息。

```
<Sysname> display qos trust interface ethernet 1/1
Interface: Ethernet1/1
 Port priority trust information
  Port priority:4
  Port priority trust type: dot1p,
```

表2-2 display qos trust interface 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号构成
Port priority trust information	端口优先级信任信息
Port priority	端口优先级
Port priority trust type	端口优先级信任类型，可能的取值为**dot1p**

2.3.2 qos trust

【命令】

qos trust { **dot1p** | **dscp** }

undo qos trust

【视图】

二层以太网接口视图/端口组视图

【缺省级别】

2：系统级

【参数】

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，以此优先级进行优先级映射。

MSR 系列路由器各款型对于本节所描述的命令及参数的支持情况有所不同，详细差异信息如下：

型号	命令	参数	描述
MSR 900	qos trust	dscp	不支持
MSR 930			支持
MSR 20-1X			不支持
MSR 20			不支持
MSR 30			仅30-11E、30-11F支持
MSR 50			不支持
MSR 2600			支持

【描述】

qos trust 命令用来配置端口优先级信任模式。**undo qos trust** 命令用来恢复端口优先级信任模式为缺省值。

【举例】

在以太网端口 Ethernet1/1 上配置优先级信任模式为信任报文自带的 802.1p 优先级。

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] qos trust dot1p
```

3 流量监管/流量整形/物理接口限速

3.1 流量监管配置命令

3.1.1 display qos car interface

【命令】

display qos car interface [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

interface-type interface-number：指定的接口类型和接口编号。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display qos car interface 命令用来显示 CAR 在指定接口上的参数设置情况和运行统计信息。

如不指定接口，本命令将显示所有接口的 CAR 参数设置情况和运行统计信息。

如指定接口为 Virtual-Template 接口，将显示继承该 Virtual-Template 接口的所有 Virtual-Access 接口下的 QoS CAR 的信息，Virtual-Template 本身无 QoS 信息显示。

【举例】

显示 CAR 在 Ethernet1/1 接口上的参数设置情况和运行统计信息。

```
<Sysname> display qos car interface ethernet1/1
Interface: Ethernet1/1
Direction: Inbound
  Rule(s): If-match Any
  CIR 10 (kbps),  CBS 2000 (byte),  EBS 0 (byte)
  Green Action: pass
  Red Action : discard
  Green : 0(Packets) 0(Bytes)
  Red   : 0(Packets) 0(Bytes)
Direction: Outbound
  Rule(s): If-match ACL  2002
```

```
CIR 10 (kbps),  CBS 1875 (byte),  EBS 0 (byte)
Green Action: pass
Red Action : discard
Green : 0(Packets) 0(Bytes)
Red   : 0(Packets) 0(Bytes)
```

表3-1 display qos car 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号结合在一起组成
Direction	指定流量监管的方向
Rule(s)	数据包的匹配规则
CIR	承诺信息速率，单位为kbps
CBS	承诺突发尺寸，也就是容纳突发流量的令牌桶深度，单位为byte
EBS	超出突发尺寸，在双令牌桶算法中超出承诺突发流量的部分，单位为byte
Green Action	对速率低于CIR的数据包的操作
Red Action	对超出的数据包的操作
Green	速率低于CIR的数据包数目和字节数
Red	超出的数据包数目和字节数

3.1.2 display qos carl

【命令】

display qos carl [*carl-index*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

carl-index：CAR 列表的号码，取值范围为 1～199。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display qos carl 命令用来显示 CAR 列表的某条规则或所有规则。

如不指定 *carl-index*，本命令将显示所有的 CAR 列表的规则。

【举例】

显示 CAR 列表的第一条规则。

```
<Sysname> display qos carl 1
Current CARL Configuration:
List  Params
------------------------------------------------------
1     MAC Address 0001-0001-0001
```

表3-2 display qos carl 命令显示信息描述表

字段	描述
List	规则编号
Params	数据包的匹配规则

3.1.3 qos car (interface view, port group view)

【命令】

qos car { **inbound** | **outbound** } { **any** | **acl** [**ipv6**] *acl-number* | **carl** *carl-index* } **cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**green** *action*] [**red** *action*]

undo qos car { **inbound** | **outbound** } { **any** | **acl** [**ipv6**] *acl-number* | **carl** *carl-index* }

【视图】

接口视图/端口组视图

【缺省级别】

2：系统级

【参数】

inbound：对接口接收到的数据包进行限速。

outbound：对接口发送的数据包进行限速。

any：对所有的 IP 数据包进行限速。

acl *acl-number*：对匹配 IPv4 ACL 的数据包进行限速。*acl-number* 为 IPv4 ACL 编号。

acl ipv6 *acl-number*：对匹配 IPv6 ACL 的数据包进行限速。*acl-number* 为 IPv6 ACL 编号。

carl *carl-index*：对匹配 CAR 列表的数据包进行限速。*carl-index* 为承诺访问速率列表编号，取值范围为 1～199。

cir *committed-information-rate*：承诺信息速率，单位为 kbps。

cbs *committed-burst-size*：承诺突发尺寸，实际平均速率在承诺速率以内时的突发流量，单位为 byte。

ebs *excess-burst-size*：过度突发尺寸，单位为 byte，缺省值为 0byte。

green：数据流量符合承诺速率时对数据包采取的动作，缺省动作为 **pass**。

red：数据流量不符合承诺速率时对数据包采取的动作，缺省动作为 **discard**。

action：对数据包采取的动作，有以下几种：

- **continue**：继续由下一个 CAR 策略处理。
- **discard**：丢弃数据包。
- **pass**：允许数据包通过。
- **remark-dscp-continue** *new-dscp*：设置报文新的 DSCP 值，并继续由下一个 CAR 策略处理，取值范围为 0～63；用文字表示时，可以选取 **af11**、**af12**、**af13**、**af21**、**af22**、**af23**、**af31**、**af32**、**af33**、**af41**、**af42**、**af43**、**cs1**、**cs2**、**cs3**、**cs4**、**cs5**、**cs6**、**cs7**、**default**、**ef**。
- **remark-dscp-pass** *new-dscp*：设置报文新的 DSCP 值，并允许数据包通过，取值范围为 0～63；用文字表示时，可以选取 **af11**、**af12**、**af13**、**af21**、**af22**、**af23**、**af31**、**af32**、**af33**、**af41**、**af42**、**af43**、**cs1**、**cs2**、**cs3**、**cs4**、**cs5**、**cs6**、**cs7**、**default**、**ef**。
- **remark-prec-continue** *new-precedence*：设置新的 IP 优先级，并继续由下一个 CAR 策略处理，取值范围为 0～7。
- **remark-prec-pass** *new-precedence*：设置新的 IP 优先级，并允许数据包通过，取值范围为 0～7。

【描述】

qos car 命令用来在某个接口实施 CAR 策略。**undo qos car** 命令用来删除接口上的某个 CAR 策略。

该命令的重复执行将在接口上配置多个 CAR 策略，策略的执行顺序与配置的先后顺序一致。

在接口视图下执行该命令，则该配置只在当前接口生效；在端口组视图下执行该命令，则该配置将在端口组中的所有端口生效。

【举例】

在接口 Ethernet1/1 的出方向上对满足 CARL 规则 1 的报文进行流量监管。报文正常流速为 200kbps，在第一时间可以有 2 倍于正常流量的突发流量通过，以后速率小于等于 200kbps 时正常发送，大于 200kbps 时，报文优先级改为 0 并发送。

```
<Sysname> system-view
[Sysname] interface ethernet1/1
[Sysname-Ethernet1/1] qos car outbound carl 1 cir 200 cbs 50000 ebs 0 green pass red
remark-prec-pass 0
```

3.1.4 qos carl

【命令】

qos carl *carl-index* { **precedence** *precedence-value* | **mac** *mac-address* | **dscp** *dscp-list* | { **destination-ip-address** | **source-ip-address** } { **subnet** *ip-address mask-length* | **range** *start-ip-address* **to** *end-ip-address* } [**per-address** [**shared-bandwidth**]] }

undo qos carl *carl-index*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

carl-index：CAR 列表号码，取值范围为 1～199。

precedence *precedence-value*：优先级，取值范围为 0～7。

mac *mac-address*：16 进制的 MAC 地址。

dscp *dscp-list*：DSCP 取值列表。DSCP 为区分服务编码点，用数字表示时，取值范围为 0～63；用文字表示时，可以选取 **af11**、**af12**、**af13**、**af21**、**af22**、**af23**、**af31**、**af32**、**af33**、**af41**、**af42**、**af43**、**cs1**、**cs2**、**cs3**、**cs4**、**cs5**、**cs6**、**cs7**、**default**、**ef**。

destination-ip-address：基于目的 IP 地址的 CAR 列表。

source-ip-address：基于源 IP 地址的 CAR 列表。

subnet *ip-address mask-length*：IP 子网地址和 IP 子网地址掩码长度。

range *start-ip-address* **to** *end-ip-address*：IP 地址段起始地址和 IP 地址段终止地址。*end-ip-address* 必须大于 *start-ip-addres*。

per-address：表示对网段内逐 IP 地址流量进行限速。如果不选择该参数，表示对整个网段的流量进行限速。

shared-bandwidth：表示网段内各 IP 地址的流量共享剩余带宽。

【描述】

qos carl 命令用来创建或修改 CAR 自身的规则列表。**undo qos carl** 命令用来删除 CAR 列表。

可以选择基于优先级、基于 MAC 地址、基于 DSCP 或基于 IP 网段建立 CAR 列表。

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

可以配置多个 **precedence** 值，最多可指定 8 个；如果指定了多个相同的 **precedence** 值，系统默认为一个；多个不同的 **precedence** 值是或的关系，即只要有一个值匹配，就算匹配这条规则。

可以配置多个 DSCP 值，最多可指定 8 个；如果指定了多个相同的 DSCP 值，系统默认为一个；多个不同的 DSCP 值是或的关系，即只要有一个值匹配，就算匹配这条规则。

指定单个 IP 地址限速请使用接口视图下 **qos car acl** 命令配置。

注意

基于 IP 网段类型的 CAR 列表:

- 如果未指定 **per-address**，则应用该 CAR 列表到接口时，**cir** 为该网段内所有 IP 地址带宽之和，各个 IP 地址带宽按照流量大小的比例进行分配;
- 如果指定 **per-address** 未指定 **shared-bandwidth**，则应用该 CAR 列表到接口时，**cir** 为各 IP 地址独享的限制带宽，不能被网段内其他 IP 流量共享;
- 如果指定 **per-address** 和 **shared-bandwidth**，则应用该 CAR 列表到接口时，**cir** 为该网段内所有 IP 地址共享带宽之和，根据当前存在流量的 IP 地址数量，动态平均分配各 IP 地址占用的带宽。

例如，应用 192.168.0.1 到 192.168.0.100 的逐地址限速 CAR 列表到接口，总带宽为 10Mbps，如果指定 **shared-bandwidth** 则 **cir** 配置为 10Mbps；如果未指定 **shared-bandwidth** 则 **cir** 配置为 100kbps。

【举例】

下面的命令将配置 CAR 规则 1 为报文优先级 7。

```
<Sysname> system-view
[Sysname] qos carl 1 precedence 7
```

在接口 Ethernet1/1 的出方向上应用 CARL 规则 1。CARL 规则 1 是对源地址属于子网 1.1.1.0/24 内每台 PC 限速 100kbps，网段内各 IP 地址的流量不共享剩余带宽。

```
<Sysname> system-view
[Sysname] qos carl 1 source-ip-address subnet 1.1.1.0 24 per-address
[Sysname] interface ethernet1/1
[Sysname-Ethernet1/1] qos car outbound carl 1 cir 100 cbs 6250 ebs 0 green pass red discard
```

在接口 Ethernet1/1 的出方向上应用 CARL 规则 2。CARL 规则 2 是对源地址属于 IP 地址段 1.1.2.100～1.1.2.199 内所有 PC 限速 5Mbps，网段内各 IP 地址的流量共享剩余带宽。

```
<Sysname> system-view
[Sysname] qos carl 2 source-ip-address range 1.1.2.100 to 1.1.2.199 per-address
shared-bandwidth
[Sysname] interface ethernet1/1
[Sysname-Ethernet1/1] qos car outbound carl 2 cir 5000 cbs 3125 ebs 31250 green pass red
discard
```

3.2 流量整形配置命令

3.2.1 display qos gts interface

【命令】

display qos gts interface [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

interface-type interface-number：指定的接口类型和接口编号。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display qos gts interface 命令用来显示指定接口或所有接口的 GTS 配置情况和统计信息。

如不指定接口，本命令将显示所有接口的 GTS 配置情况和运行统计信息。

如指定接口为 Virtual-Template 接口，将显示继承该 Virtual-Template 接口的所有 Virtual-Access 接口下的 QoS GTS 的信息，Virtual-Template 本身无 QoS 信息显示。

【举例】

显示所有接口的 GTS 配置情况和统计信息。

```
<Sysname> display qos gts interface
 Interface: Ethernet1/1
 Rule(s): If-match ACL  2001
 CIR 200 (kbps), CBS 50000 (byte), EBS 0 (byte)
 Queue Length: 100 (Packets)
 Queue Size: 70 (Packets)
 Passed   : 0(Packets) 0(Bytes)
 Discarded: 0(Packets) 0(Bytes)
 Delayed  : 0(Packets) 0(Bytes)
```

表3-3 display qos gts 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号结合在一起组成
Rule(s)	匹配规则。可以是三种类型中的任意一种
CIR	承诺信息速率，单位为kbps
CBS	承诺突发尺寸，也就是容纳突发流量的令牌桶深度，单位为byte
EBS	超出突发尺寸，在双令牌桶算法中超出承诺突发流量的部分，单位为byte
Queue Length	缓冲队列能够容纳的数据包的个数
Queue Size	当前缓冲区中数据包的数目
Passed	已经通过的数据包数目和字节数
Discarded	被丢弃的数据包数目和字节数
Delayed	被延迟发送的数据包数目和字节数

3.2.2 qos gts

【命令】

qos gts { **any** | **acl** *acl-number* } **cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*] [**queue-length** *queue-length*]]

undo qos gts { **any** | **acl** *acl-number* }

【视图】

接口视图/端口组视图

【缺省级别】

2：系统级

【参数】

any：对所有的数据包进行流量整形。

acl *acl-number*：对匹配访问控制列表的数据包进行流量整形。*acl-number* 为访问控制列表编号。

cir *committed-information-rate*：承诺信息速率。

cbs *committed-burst-size*：承诺突发尺寸，单位为 kbps。

ebs *excess-burst-size*：超出突发尺寸，在双令牌桶算法中超出承诺突发流量的部分，单位为 byte。缺省取值为 0，即只采用一个令牌桶监管，单位为 kbps。

queue-length *queue-length*：缓存队列的最大长度，缺省取值为 50。

【描述】

qos gts 命令用来为某一类别的流或接口下所有流设置整形参数，并开始整形。**undo qos gts** 命令用来取消对某一类流或接口下所有流的整形设置。

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

qos gts any 用来为接口下所有的流设置整形参数。

缺省情况下，接口上没有配置整形参数。

在接口视图下执行该命令，则该配置只在当前接口生效；在端口组视图下执行该命令，则该配置将在端口组中的所有端口生效。

说明

接口下的 qos gts 命令不支持配置 IPv6 的 ACL 参数，如果需要用 IPv6 的 ACL 进行流量整形，请用 QoS 策略的方式配置。

相关配置可参考命令 **acl**。

【举例】

下面的命令将在接口 Ethernet1/1 上对满足 ACL 规则 2001 的报文进行流量整形。正常流速为 200kbps，在第一时间可以有 2 倍于正常流量的突发流量（50000bytes）通过，以后速率小于等于 200kbps 时正常发送，速率大于 200kbps 时，将进入缓存队列，缓存队列长度为 100。

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] qos gts acl 2001 cir 200 cbs 50000 ebs 0 queue-length 100
```

3.3 物理接口限速配置命令

3.3.1 display qos lr interface

【命令】

display qos lr interface [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

interface-type interface-number：指定的接口类型和接口编号。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display qos lr interface 命令用来显示某个或者全部接口的 LR 配置情况和统计信息。

如不指定接口，本命令将显示所有接口的 LR 配置情况和运行统计信息。

如指定接口为 Virtual-Template 接口，将显示继承该 Virtual-Template 接口的所有 Virtual-Access 接口下的 QoS LR 的信息，Virtual-Template 本身无 QoS 信息显示。

【举例】

显示所有接口的 LR 配置情况和统计信息。

```
<Sysname> display qos lr interface
Interface: Ethernet1/1
Direction: Outbound
 CIR 10 (kbps),  CBS 1875 (byte),  EBS 0 (byte)
Passed : 0(Packets) 0(Bytes)
 Delayed: 0(Packets) 0(Bytes)
 Active Shaping: NO
Direction: Inbound
 CIR 10 (kbps),  CBS 1875 (byte),  EBS 0 (byte)
Passed : 0(Packets) 0(Bytes)
 Delayed: 0(Packets) 0(Bytes)
 Active Shaping: NO
```

表3-4 display qos lr 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号结合在一起组成
Direction	指明物理接口限速的方向是入接口还是出接口
CIR	承诺信息速率，单位为kbps
CBS	承诺突发尺寸，也就是容纳突发流量的令牌桶深度，单位为byte
EBS	超出突发尺寸，在双令牌桶算法中超出承诺突发流量的部分，单位为byte
Passed	已经通过的数据包数目和字节数
Delayed	被延迟发送的数据包数目和字节数

字段	描述
Active Shaping	当前限速配置是否被激活

3.3.2 qos lr

【命令】

qos lr { **inbound** | **outbound** } **cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]]

undo qos lr { **inbound** | **outbound** }

【视图】

接口视图/端口组视图

【缺省级别】

2：系统级

【参数】

inbound：对接口接收的数据流进行限速。

outbound：对接口发送的数据流进行限速。

cir *committed-information-rate*：承诺信息速率。

cbs *committed-burst-size*：承诺突发尺寸，缺省取值为 500 毫秒以 CIR 速率通过的流量。

ebs *excess-burst-size*：超出突发尺寸，在双令牌桶算法中超出承诺突发流量的部分，单位为 byte。缺省取值为 0，即只采用一个令牌桶监管。

【描述】

qos lr 命令用来限制物理接口的接收或者发送数据的速率。**undo qos lr** 命令用来取消限制。

在接口视图下执行该命令，则该配置只在当前接口生效；在端口组视图下执行该命令，则该配置将在端口组中的所有端口生效。

MSR 系列路由器各款型对于本节所描述的命令及参数的支持情况有所不同，详细差异信息如下：

型号	命令	参数	描述
MSR 900	**qos lr**	**inbound**	不支持
MSR 930			不支持
MSR 20-1X			不支持
MSR 20			不支持
MSR 30			MSR 30-11E、30-11F固定二层以太网接口支持 MIM-16FSW、DMIM-24FSW二层以太网交换接口模块支持
MSR 50			FIC-16FSW、DFIC-24FSW二层以太网交换接口模块支持
MSR 2600			不支持

【举例】

下面的命令将对物理接口 Ethernet1/1 发出的报文进行限速，正常流速 20kbps，承诺突发流量是 2000bytes，超出突发流量是 0。

```
<Sysname> system-view
[Sysname] interface ethernet1/1
[Sysname-Ethernet1/1] qos lr outbound cir 20 cbs 2000 ebs 0
```

4 拥塞管理

4.1 FIFO队列配置命令

4.1.1 qos fifo queue-length

【命令】

qos fifo queue-length *queue-length*

undo qos fifo queue-length

【视图】

接口视图/PVC 视图

【缺省级别】

2：系统级

【参数】

queue-length：队列的长度限制，取值范围为 1～1024，队列的缺省长度限制为 75。

【描述】

qos fifo queue-length 命令用来配置先进先出队列的长度。**undo qos fifo queue-length** 命令用来恢复先进先出队列的长度为缺省值。

注意

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 功能以保证队列生效。

【举例】

下面命令把 FIFO 的队列长度设置为 100。

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] qos fifo queue-length 100
```

4.2 优先级队列配置命令

4.2.1 display qos pq interface

【命令】

display qos pq interface [*interface-type interface-number* [**pvc** { *pvc-name* [*vpi/vci*] | *vpi/vci* }]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

interface-type interface-number：指定的接口类型和接口编号。

pvc { *pvc-name* [*vpi/vci*] | *vpi/vci* }：只用于 ATM 接口，即可显示指定 ATM 接口上的指定 PVC 的信息。*pvc-name* 表示 PVC 名。*vpi/vci* 表示 VPI/VCI 值。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display qos pq interface 命令用来显示指定接口、指定 PVC 或所有接口及 PVC 的优先级队列配置情况和统计信息。

如不指定接口或 PVC，本命令将显示所有接口及 PVC 的优先级队列配置情况和统计信息。

如指定接口为 Virtual-Template 接口，将显示继承该 Virtual-Template 接口的所有 Virtual-Access 接口下的 QoS PQ 的信息，Virtual-Template 本身无 QoS 信息显示。

相关配置可参考命令 **qos pq**。

【举例】

显示 Ethernet1/1 接口的优先级队列配置情况和统计信息。

```
<Sysname> display qos pq interface ethernet 1/1
Interface: Ethernet1/1
Output queue : (Urgent queuing : Size/Length/Discards)  0/100/0
Output queue : (Protocol queuing : Size/Length/Discards)  0/500/0
Output queue : (Priority queuing : PQL 1 Size/Length/Discards)
Top:  0/20/0    Middle:  0/40/0    Normal:  0/60/0    Bottom:  0/80/0
```

表4-1 display pq interface 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号结合在一起组成
Output queue	出队列信息
Urgent queuing	紧急队列
Protocol queuing	协议队列
Priority queuing	优先级队列，指明使用哪一条优先级队列列表
Size	队列中数据包数目

字段	描述
Length	队列大小
Discards	丢弃的数据包数目
Top	高优先级队列
Middle	中优先级队列
Normal	普通优先级队列
Bottom	低优先级队列

4.2.2 display qos pql

【命令】

display qos pql [*pql-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

pql-number：优先级队列列表的序号。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display qos pql 命令用来显示指定或者所有优先级队列列表的内容。

本命令不显示使用缺省配置的项。

相关配置可参考命令 **qos pq pql** 和 **qos pq**。

【举例】

显示优先列表。

```
<Sysname> display qos pql
Current PQL Configuration:
List  Queue   Params
------------------------------------------------------
1     Top     Protocol ip less-than 1000
2     Normal  Length 60
2     Bottom  Length 40
```

```
3     Middle  Inbound-interface Ethernet1/1
4     Top     Local-precedence  7
```

4.2.3 qos pq

【命令】

qos pq pql *pql-index*

undo qos pq

【视图】

接口视图/PVC 视图

【缺省级别】

2：系统级

【参数】

pql：采用指定的优先级队列列表中定义的参数。

pql-index：优先列表的组号，取值范围为 1～16。

【描述】

qos pq 命令用来在接口上应用优先级队列调度机制。**undo qos pq** 命令用来将接口的拥塞管理策略恢复到 FIFO。

缺省情况下，各接口拥塞管理策略为 FIFO。

除链路层协议为 X.25、LAPB 协议的接口外，所有物理接口都可以应用优先级队列。

一个接口只能应用一组优先级队列列表。

可以为优先列表的组配置多条分类规则。在进行流分类的时候，系统沿规则链进行匹配，如果匹配上某规则则进入相应的队列，匹配结束；如果数据包不与任何规则匹配，则进入缺省队列。

注意

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 功能以保证队列生效。

相关配置可参考命令 **qos pql**、**display qos pq interface**、**display qos pql** 和 **display interface**。

【举例】

将第 12 组优先列表应用到 Ethernet1/1 上。

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] qos pq pql 12
```

4.2.4 qos pql default-queue

【命令】

qos pql *pql-index* **default-queue** { **bottom** | **middle** | **normal** | **top** }

undo qos pql *pql-index* **default-queue**

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

pql-index：优先列表的组号，取值范围为 1～16。

top、**middle**、**normal**、**bottom**：对应 PQ 的四个队列，优先级依次降低。缺省情况下，队列为 **normal**。

【描述】

qos pql default-queue 命令用来将那些无对应规则的包指定到一个缺省队列。**undo qos pql default-queue** 命令用来取消配置，恢复缺省值。

进行流分类时，如果数据包不与任何规则匹配，则进入缺省队列。

对于同一个 *pql-index*，该命令重复使用将设定新的缺省队列。

相关配置可参考命令 **qos pql inbound-interface**、**qos pql protocol**、**qos pql queue** 和 **qos pq**。

【举例】

将优先列表中第 12 组中无对应规则的包的缺省队列设定为 bottom。

```
<Sysname> system-view
[Sysname] qos pql 12 default-queue bottom
```

4.2.5 qos pql inbound-interface

【命令】

qos pql *pql-index* **inbound-interface** *interface-type interface-number* **queue** { **bottom** | **middle** | **normal** | **top** }

undo qos pql *pql-index* **inbound-interface** *interface-type interface-number*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

pql-index：优先级队列的组号，取值范围为 1～16。

interface-type interface-number：指定的接口类型和接口编号。

top、**middle**、**normal**、**bottom**：对应 PQ 的四个队列，优先级依次降低。

【描述】

qos pql inbound-interface 命令用来建立基于接口的分类规则。**undo qos pql inbound-interface** 命令用来删除相应的分类规则。

缺省情况下，不配置任何分类规则。

该命令按报文输入的接口进行匹配。对于同一个 *pql-index*，该命令可以重复使用，为来自不同接口的报文建立不同的分类规则。

相关配置可参考命令 **qos pql default-queue**、**qos pql protocol**、**qos pql queue** 和 **qos pq**。

【举例】

指定规则 12，使得来自 Serial2/0 的报文进入 **middle** 队列。

```
<Sysname> system-view
[Sysname] qos pql 12 inbound-interface serial 2/0 queue middle
```

4.2.6 qos pql protocol

【命令】

qos pql *pql-index* **protocol ip** [*queue-key key-value*] **queue** { **bottom** | **middle** | **normal** | **top** }

undo qos pql *pql-index* **protocol ip** [*queue-key key-value*]

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

pql-index：优先列表的组号，取值范围为 1～16。

top、**middle**、**normal**、**bottom**：对应 PQ 的四个队列，优先级依次降低。

ip [*queue-key key-value*]：表示将 IP 报文分类进入队列。*queue-key* 和 *key-value* 的取值见下表。当不输入 *queue-key* 和 *key-value* 时，表示所有 IP 报文进入队列。

表4-2 queue-key 和 key-value 的取值

queue-key	*key-value*	意义
acl	access-list-number（2000～3999）	符合某访问控制列表定义的IP报文就进入队列
fragments	-	只要是分片的IP报文就进入队列
greater-than	长度值（0～65535）	长度大于某个计数值的IP报文进入队列
less-than	长度值（0～65535）	长度小于某个计数值的IP报文进入队列
tcp	端口号（0～65535）	只要IP报文的源或目的TCP端口号为指定的端口号，就进入队列
udp	端口号（0～65535）	只要IP报文的源或目的UDP端口号为指定的端口号，就进入队列

注意

当 *queue-key* 指定为 tcp 或 udp 时，*key-value* 的值既可以直接使用端口名称，也可以使用相关端口号。

【描述】

qos pql protocol 命令用来建立基于协议的分类规则。**undo qos pql protocol** 命令用来删除相应的分类规则。

缺省情况下，设备上没有配置任何规则。

设备是以规则被配置的顺序来匹配数据包，如果发现数据包与某个规则匹配，便结束整个查找过程。

对于同一个 *pql-index*，该命令可以重复使用，为 IP 数据包建立多种分类规则。

相关配置可参考命令 **qos pql default-queue**、**qos pql inbound-interface**、**qos pql queue** 和 **qos pq**。

【举例】

指定 PQ 规则 1，使满足 ACL 为 3100 规则定义的 IP 报文进入 **top** 队列。

```
<Sysname> system-view
[Sysname] qos pql 1 protocol ip acl 3100 queue top
```

4.2.7 qos pql queue

【命令】

qos pql *pql-index* **queue** { **bottom** | **middle** | **normal** | **top** } **queue-length** *queue-length*

undo qos pql *pql-index* **queue** { **bottom** | **middle** | **normal** | **top** } **queue-length**

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

pql-index：优先列表的组号，取值范围为 1～16。

queue-length：为不同级别优先级队列组的长度值，取值范围为 1～1,024。

各优先级队列组长度的缺省值如下：

- 顶层队列的缺省长度值为 20；
- 中间队列的缺省长度值为 40；
- 一般队列的缺省长度值为 60；
- 底层队列的缺省长度值为 80。

【描述】

qos pql queue 命令用来设置 PQ 各队列的长度（所能容纳的数据包个数）。**undo qos pql queue** 命令用来恢复各队列长度的缺省值。

如果某一队列满，新来的属于该队列的数据包就要被丢弃。

相关配置可参考命令 **qos pql default-queue**、**qos pql inbound-interface**、**qos pql protocol** 和 **qos pq**。

【举例】

指定优先列表第 10 组 **top** 队列的长度为 10。

```
<Sysname> system-view
[Sysname] qos pql 10 queue top queue-length 10
```

4.3 定制队列配置命令

4.3.1 display qos cq interface

【命令】

display qos cq interface [*interface-type interface-number* [**pvc** { *pvc-name* [*vpi/vci*] | *vpi/vci* }]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

interface-type interface-number：指定的接口类型和接口编号。

pvc { *pvc-name* [*vpi/vci*] | *vpi/vci* }：只用于 ATM 接口，即可显示指定 ATM 接口上的指定 PVC 的信息。*pvc-name* 表示 PVC 名。*vpi/vci* 表示 VPI/VCI 值。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display qos cq interface 命令用来显示指定接口、指定 PVC 或所有接口及 PVC 上的定制队列配置情况和统计信息。

如果不指定接口，本命令将显示所有接口的 CQ 配置情况和统计信息。

如指定接口为 Virtual-Template 接口，将显示继承该 Virtual-Template 接口的所有 Virtual-Access 接口下的 QoS CQ 的信息，Virtual-Template 本身无 QoS 信息显示。

相关配置可参考命令 **qos cq**。

【举例】

显示接口 Ethernet1/1 的定制队列配置情况和统计信息。

```
<Sysname> display qos cq interface ethernet 1/1
Interface: Ethernet1/1
Output queue : (Urgent queuing : Size/Length/Discards)  0/100/0
Output queue : (Protocol queuing : Size/Length/Discards)  0/500/0
Output queue : (Custom queuing : CQL 1 Size/Length/Discards)
 1:   0/  20/0          2:   0/  20/0          3:   0/  20/0
 4:   0/  20/0          5:   0/  20/0          6:   0/  20/0
 7:   0/  20/0          8:   0/  20/0          9:   0/  20/0
```

```
10:    0/  20/0          11:    0/  20/0          12:    0/  20/0
13:    0/  20/0          14:    0/  20/0          15:    0/  20/0
16:    0/  20/0
```

表4-3 display qos cq interface 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号结合在一起组成
Output queue	出队列信息
Urgent queuing	紧急队列
Protocol queuing	协议队列
Custom queuing	定制队列，指明使用哪一条定制队列列表
Size	队列中数据包数目
Length	队列大小
Discards	丢弃的数据包数目

4.3.2 display qos cql

【命令】

display qos cql [*cql-index*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

cql-index：定制列表的组号，取值范围为 1～16。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display qos cql 命令用来显示定制列表的内容。

如果为缺省值，则不被显示。如果不指定定制列表的组号，则显示所有列表的内容。

相关配置可参考命令 **qos cq** 和 **qos cql**。

【举例】

显示所有定制列表的内容。

```
<Sysname> display qos cql
Current CQL Configuration:
-------------------------------------------------------
List  Queue  Params
2     3      Protocol ip fragments
3     6      Length 100
3     1      Inbound-interface Ethernet1/1
4     5      Local-precedence  7
```

4.3.3 qos cq

【命令】

qos cq cql *cql-index*

undo qos cq

【视图】

接口视图/PVC 视图

【缺省级别】

2：系统级

【参数】

cql-index：定制列表的组号，取值范围为 1～16。

【描述】

qos cq 命令用来在接口上应用定制队列。**undo qos cq** 命令用来将接口的拥塞管理策略恢复到 FIFO。

缺省情况下，接口拥塞管理策略为 FIFO。

除链路层协议为 X.25、LAPB 协议的接口外，所有物理接口都可以应用定制队列。

一个接口只能应用一组定制队列。

我们可以为定制列表的组配置多条分类规则。在进行流分类的时候，系统沿规则链进行匹配，如果匹配上某规则则进入相应的队列，匹配结束；如果数据包不与任何规则匹配，则进入缺省队列。

注意

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 功能以保证队列生效。

相关配置可参考命令 **qos cql default-queue**、**qos cql inbound-interface**、**qos cql protocol**、**qos cql queue serving** 和 **qos cql queue**。

【举例】

将定制列表的第 5 组应用到 Ethernet1/1 上。

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
```

```
[Sysname-Ethernet1/1] qos cq cql 5
```

4.3.4 qos cql default-queue

【命令】

qos cql *cql-index* **default-queue** *queue-number*

undo qos cql *cql-index* **default-queue**

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

cql-index：定制列表的组号，取值范围为 1～16。

queue-number：队列号，取值范围为 1～16，缺省队列号为 1。

【描述】

qos cql default-queue 命令用来为那些无对应规则的包指定一个缺省队列。**undo qos cql default-queue** 命令用来取消配置，恢复缺省值。

在进行流分类的时候，如果数据包不与任何规则匹配，则进入缺省队列。

相关配置可参考命令 **qos cql inbound-interface**、**qos cql protocol**、**qos cql queue serving**、**qos cql queue** 和 **qos cq**。

【举例】

指定定制列表第 5 组的缺省队列为 2。

```
<Sysname> system-view
[Sysname] qos cql 5 default-queue 2
```

4.3.5 qos cql inbound-interface

【命令】

qos cql *cql-index* **inbound-interface** *interface-type interface-number* **queue** *queue-number*

undo qos cql *cql-index* **inbound-interface** *interface-type interface-number*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

cql-index：定制列表的组号，取值范围为 1～16。

interface-type interface-number：指定的接口类型和接口编号。

queue-number：队列号，取值范围为 1～16。

【描述】

qos cql inbound-interface 命令用来建立基于接口的分类规则。**undo qos cql inbound-interface** 命令用来删除相应的分类规则。

缺省情况下，不配置任何分类规则。

该命令按报文输入的接口进行匹配。对于同一个 *cql-index*，该命令可以重复使用，为来自不同接口的报文建立不同的分类规则。

相关配置可参考命令 **qos cql default-queue**、**qos cql protocol**、**qos cql queue serving** 和 **qos cql queue**。

【举例】

指定了一条规则 5 使得来自于 Ethernet1/1 的报文进入队列 3。

```
<Sysname> system-view
[Sysname] qos cql 5 inbound-interface ethernet 1/1 queue 3
```

4.3.6 qos cql protocol

【命令】

qos cql *cql-index* **protocol ip** [*queue-key key-value*] **queue** *queue-number*

undo qos cql *cql-index* **protocol ip** [*queue-key key-value*]

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

cql-index：定制列表的组号，取值范围为 1～16。

queue *queue-number*：定制队列的队列号，取值范围为 1～16。

ip [*queue-key key-value*]：表示将 IP 报文分类进入队列。*queue-key* 和 *key-value* 的取值见下表。当不输入 *queue-key* 和 *key-value* 时，表示所有 IP 报文进入队列。

表4-4 queue-key 和 key-value 的取值

queue-key	*key-value*	意义
acl	access-list-number（2000~3999）	符合某访问控制列表定义的IP报文就进入队列
fragments	-	只要是分片的IP报文就进入队列
greater-than	长度值（0~65535）	长度大于某个计数值的IP报文进入队列
less-than	长度值（0~65535）	长度小于某个计数值的IP报文进入队列
tcp	端口号（0~65535）	只要IP报文的源或目的TCP端口号为指定的端口号，就进入队列
udp	端口号（0~65535）	只要IP报文的源或目的UDP端口号为指定的端口号，就进入队列

说明

当 *queue-key* 指定为 tcp 或 udp 时，*key-value* 的值既可以直接使用端口名称，也可以使用相关端口号。

【描述】

qos cql protocol 命令用来配置基于协议的分类规则。**undo qos cql protocol** 命令用来删除相应的分类规则。

系统是以规则被配置的顺序来匹配数据包，如果发现数据包与某个规则匹配，便结束整个查找过程。

对于同一个 *cql-index*，该命令可以重复使用，为 IP 数据包建立多种分类规则。

缺省情况下，不配置任何分类规则。

相关配置可参考命令 **qos cql default-queue**、**qos cql inbound-interface**、**qos cql queue** 和 **qos cq cql**。

【举例】

指定 CQ 规则 5，使得匹配访问控制列表 3100 的 IP 报文进入队列 3。

```
<Sysname> system-view
[Sysname] qos cql 5 protocol ip acl 3100 queue 3
```

4.3.7 qos cql queue

【命令】

qos cql *cql-index* **queue** *queue-number* **queue-length** *queue-length*

undo qos cql *cql-index* **queue** *queue-number* **queue-length**

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

cql-index：定制列表的组号，取值范围为 1～16。

queue-number：队列号，取值范围为 1～16。

queue-length *queue-length*：队列的最大长度，取值范围为 1～1024，缺省值为 20。

【描述】

qos cql queue 命令用来设置各队列的长度（所能容纳的数据包个数）。**undo qos cql queue** 命令用来恢复队列长度的缺省值。

如果队列已满，新来的数据包就要被丢弃。

相关配置可参考命令 **qos cql default-queue**、**qos cql inbound-interface**、**qos cql protocol**、**qos cql queue serving** 和 **qos cq**。

【举例】

指定定制列表第 5 组队列 4 的长度为 40。

```
<Sysname> system-view
[Sysname] qos cql 5 queue 4 queue-length 40
```

4.3.8 qos cql queue serving

【命令】

qos cql *cql-index* **queue** *queue-number* **serving** *byte-count*

undo qos cql *cql-index* **queue** *queue-number* **serving**

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

cql-index：定制列表的组号，取值范围为 1～16。

queue-number：队列号，取值范围为 1～16。

byte-count：队列每次轮询所发送数据包的字节数，取值范围为 1～16777215，缺省值为 1500 字节。

【描述】

qos cql queue serving 命令用来设置各队列每次轮询所发送数据包的字节数。**undo qos cql queue serving** 命令用来恢复发送数据包数的缺省值。

相关配置可参考命令 **qos cql default-queue**、**qos cql inbound-interface**、**qos cql protocol**、**qos cql queue** 和 **qos cq**。

【举例】

指定定制列表中的第 5 组队列 2 每次轮询所发送的字节数为 1400。

```
<Sysname> system-view
[Sysname] qos cql 5 queue 2 serving 1400
```

4.4 加权公平队列配置命令

4.4.1 display qos wfq interface

【命令】

display qos wfq interface [*interface-type interface-number* [**pvc** { *pvc-name* [*vpi/vci*] | *vpi/vci* }]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

interface-type interface-number：指定的接口类型和接口编号。

pvc { *pvc-name* [*vpi/vci*] | *vpi/vci* }：只用于 ATM 接口，即可显示指定 ATM 接口上的指定 PVC 的信息。*pvc-name* 表示 PVC 名。*vpi/vci* 表示 VPI/VCI 值。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display qos wfq interface 命令用来显示指定接口、指定 PVC 或所有接口及 PVC 上的加权公平队列配置情况和统计信息。

如不指定接口，本命令将显示所有接口的加权公平队列配置情况和统计信息。

如指定接口为 Virtual-Template 接口，将显示继承该 Virtual-Template 接口的所有 Virtual-Access 接口下的 QoS WFQ 的信息，Virtual-Template 本身无 QoS 信息显示。

相关配置可参考命令 **qos wfq**。

【举例】

显示接口 Ethernet1/1 的加权公平队列配置情况和统计信息。

```
<Sysname> display qos wfq interface ethernet 1/1
Interface: Ethernet1/1
Output queue : (Urgent queuing : Size/Length/Discards)  0/100/0
Output queue : (Protocol queuing : Size/Length/Discards)  0/500/0
Output queue : (Weighted Fair queuing : Size/Length/Discards)  0/64/0
Hashed by IP Precedence
Hashed queues:  0/0/128 (Active/Max active/Total)
```

表4-5 display qos wfq interface 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号结合在一起组成
Output queue	当前出队列的相关信息
Urgent queuing	紧急队列
Protocol queuing	协议队列
Weighted Fair queuing	加权公平队列
Size	队列中数据包的数目
Length	队列的长度
Discards	丢弃的数据包数目
Hashed by	权重类型，分为两类：IP Precedence和DSCP

字段	描述
Hashed queues	哈希队列的信息
Active	激活的哈希队列数目
Max active	最大激活过的哈希队列数目
Total	当前配置的哈希队列总数

4.4.2 qos wfq

【命令】

qos wfq [**dscp** | **precedence**] [**queue-length** *max-queue-length* [**queue-number** *total-queue-number*]]

undo qos wfq

【视图】

接口视图/PVC 视图

【缺省级别】

2：系统级

【参数】

dscp：区分服务编码点权重类型。

precedence：IP 优先级权重类型。

queue-length *max-queue-length*：队列的最大长度，即每个队列中可容纳的数据包的最大个数，超出后数据包将被丢弃，取值范围为 1～1024，缺省值为 64。

queue-number *total-queue-number*：队列的总数目，可取的值为：16、32、64、128、256、512、1024、2048、4096，缺省值为 256。

【描述】

qos wfq 命令用来在接口或 PVC 上应用加权公平队列或修改加权公平队列的参数。**undo qos wfq** 命令用来恢复缺省拥塞管理机制 FIFO。

除链路层协议为 X.25、LAPB 协议的接口外，所有物理接口都可以应用加权公平队列。

当不配置权重类型时，系统默认权重类型为 **precedence**。

注意

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 功能以保证队列生效。

相关配置可参考命令 **display interface** 和 **display qos wfq interface**。

【举例】

在接口 Ethernet1/1 上应用 WFQ，并设置队列长度为 100，总队列个数设置为 512 个。

```
<Sysname> system-view
[Sysname] interface ethernet1/1
[Sysname-Ethernet1/1] qos wfq queue-length 100 queue-number 512
```

4.5 基于类的队列配置命令

4.5.1 display qos cbq interface

【命令】

display qos cbq interface [*interface-type interface-number* [**pvc** { *pvc-name* [*vpi/vci*] | *vpi/vci* }]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

interface-type interface-number：指定的接口类型和接口编号。

pvc { *pvc-name* [*vpi/vci*] | *vpi/vci* }：只用于 ATM 接口，即可显示指定 ATM 接口上的指定 PVC 的信息。*pvc-name* 表示 PVC 名。*vpi/vci* 表示 VPI/VCI 值。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display qos cbq interface 命令用来显示指定接口、指定 PVC 或所有接口与 PVC 的基于类的队列配置信息和运行情况。

如果不指定接口，本命令将显示所有接口的基于类的队列配置信息和运行情况。

如指定接口为 Virtual-Template 接口，将显示继承该 Virtual-Template 接口的所有 Virtual-Access 接口下的 QoS CBQ 的信息，Virtual-Template 本身无 QoS 信息显示。

【举例】

显示所有接口与 PVC 的基于类的队列配置信息和运行情况。

```
<Sysname> display qos cbq interface
Interface: Ethernet1/1
Output queue : (Urgent queuing : Size/Length/Discards)  0/100/0
Output queue : (Protocol queuing : Size/Length/Discards)  0/500/0
Output queue : (Class Based Queuing : Size/Discards)  0/0
```

```
Queue Size:  0/0/0 (EF/AF/BE)
BE Queues:   0/0/256 (Active/Max active/Total)
AF Queues:   1 (Allocated)
Bandwidth(Kbps): 74992/75000 (Available/Max reserve)
```

表4-6 display qos cbq interface 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号结合在一起组成
Outbput queue	当前出队列的相关信息
Urgent queuing	紧急队列
Protocol queuing	协议队列
Class Based Queuing	基于类的队列
Size	队列中数据包的数目
Length	队列的长度
Discards	丢弃的数据包数目
EF	加速转发队列
AF	保证转发队列
BE	尽力转发队列
Active	BE队列当前处于激活状态的队列数
Max active	BE队列最大处于激活状态队列数
Total	BE队列总数
Bandwidth(Kbps)	带宽
Available	CBQ当前可用带宽
Max reserve	CBQ最大预留带宽

4.5.2 qos max-bandwidth

【命令】

qos max-bandwidth *bandwidth*

undo qos max-bandwidth

【视图】

接口视图

【缺省级别】

2：系统级

【参数】

bandwidth：接口最大可用带宽，取值范围为 1～1000000，单位 kbps。

【描述】

qos max-bandwidth 命令用来配置接口最大可用带宽。**undo qos max-bandwidth** 命令用来恢复接口最大可用带宽为缺省值。

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 QoS 带宽如下：

- 对于物理接口，其取值为物理接口实际的波特率或速率；
- 对于 VLAN 接口，取值为 1000000kbps；
- 对于 T1/E1、MFR、MP 等通过绑定生成的逻辑串口，其取值为绑定通道的总带宽；
- 对于 VT、Dialer、BRI、PRI 等模板类型的接口，取值为 1000000kbps；
- 对于其他虚接口（如 Tunnel 接口、HDLC 捆绑接口），取值为 0kbps；
- 对于 cellular 接口，取值为 384kbps。

说明

- 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 VT、Dialer、BRI、PRI 等主通道型接口，如果配置了 **qos max-bandwidth** 命令，af、ef 按照 **qos max-bandwidth** 的配置值进行队列带宽检测及计算，同步到 VA、B 通道等子通道类型接口上的 af、ef 也按照该值进行检测及计算，忽略子通道接口带宽，此种情况主通道接口及子通道接口 QoS 配置相同，仅输出主通道接口的提示信息；如果未配置 **qos max-bandwidth** 命令，af、ef 按照 1Gbps 带宽进行计算，同步到子通道的 af、ef 按照 VA、B 通道实际带宽进行队列计算，此种情况下，若子通道接口因带宽变化导致队列失效，将输出子通道接口提示信息。
- 对于 MP-group 和 MFR 接口，如果配置了 **qos max-bandwidth** 命令，af、ef 按照 **qos max-bandwidth** 的配置值进行队列带宽检测及计算。如果未配置 **qos max-bandwidth** 命令，当绑定子通道的总带宽足够时（子通道带宽之和乘以最大预留带宽占可用带宽的百分比的值大于等于 af、ef 的带宽之和），af、ef 按照接口的实际带宽进行计算；当绑定子通道的总带宽不够时（子通道带宽之和乘以最大预留带宽占可用带宽的百分比的值小于 af、ef 的带宽之和），af、ef 按照 1Gbps 带宽进行计算，同时输出实际带宽不够的提示信息，这种情况下不能保证队列功能有效。最大预留带宽占可用带宽的百分比可以通过命令 **qos reserved-bandwidth** 来配置。
- 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，接口需要配置该命令以提供 CBQ 的基准带宽。

【举例】

配置 Ethernet1/1 接口的最大可用带宽为 16kbps。

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] qos max-bandwidth 16
```

4.5.3 qos reserved-bandwidth

【命令】

qos reserved-bandwidth pct *percent*

undo qos reserved-bandwidth

【视图】

接口视图/PVC 视图

【缺省级别】

2：系统级

【参数】

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

【描述】

qos reserved-bandwidth 命令用来设置最大预留带宽占可用带宽的百分比。**undo qos reserved-bandwidth** 命令用来恢复缺省的配置。

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。

【举例】

设置最大预留带宽为可用带宽的 70%。

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] qos reserved-bandwidth pct 70
```

4.5.4 queue af

【命令】

queue af bandwidth { *bandwidth* | **pct** *percentage* }

undo queue af

【视图】

流行为视图

【缺省级别】

2：系统级

【参数】

bandwidth：带宽，取值范围为 8～1000000，单位 kbps。

pct *percentage*：可用带宽的百分比，取值范围为 1～100。

【描述】

queue af 命令用来配置类进行确保转发（Assured-forwarding），并配置类可确保的最小带宽。**undo queue af** 命令用来取消配置。

当在策略下将类与 **queue af** 所属行为关联时，必须满足：

- 同一个策略下为确保转发（**queue af**）和加速转发（**queue ef**）的类指定的带宽之和必须不大于该策略所应用接口的可用带宽；

- 同一个策略下为确保转发（**queue af**）和加速转发（**queue ef**）的类指定的带宽百分比之和必须不大于 100；
- 同一个策略下确保转发（**queue af**）和加速转发（**queue ef**）的类的带宽的配置必须都采用相同的值的类型，比如都采用绝对值形式，或者都采用百分比形式。

相关配置可参考命令 **qos policy**、**traffic behavior** 和 **classifier behavior**。

【举例】

为行为 database 配置确保转发，并且确保最小带宽为 200kbps。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue af bandwidth 200
```

4.5.5 queue ef

【命令】

queue ef bandwidth { *bandwidth* [**cbs** *burst*] | **pct** *percentage* [**cbs-ratio** *ratio*] }

undo queue ef

【视图】

流行为视图

【缺省级别】

2：系统级

【参数】

bandwidth：带宽，取值范围为 8～1000000，单位 kbps。

cbs *burst*：指定承诺突发尺寸，单位为字节，取值范围为 32～2000000 字节，缺省值为 *bandwidth* ×25。

pct *percentage*：可用带宽的百分比，取值范围为 1～100。

cbs-ratio *ratio*：允许的突发因子，取值范围为 25～500，默认值是 25。

【描述】

queue ef 命令用来配置加速转发（Expedited-forwarding），报文进入绝对优先级队列，并配置最大带宽。**undo queue ef** 命令用来取消配置。

本命令的注意事项如下。

- 该命令在流行为视图下不能与 **queue af**，**queue-length**，**wred** 同时使用。
- 在策略下，缺省类 default-class 不能与 **queue ef** 所属 behavior 关联。
- 同一个策略下为确保转发（**queue af**）和加速转发（**queue ef**）的类指定的带宽之和必须不大于该策略所应用接口的可用带宽。
- 同一个策略下为确保转发（**queue af**）和加速转发（**queue ef**）的类指定的带宽百分比之和必须不大于 100。
- 同一个策略下确保转发（**queue af**）和加速转发（**queue ef**）的类的带宽的配置必须都采用相同的值的类型，比如都采用绝对值形式，或者都采用百分比形式。

- 对于设置百分比形式 **queue ef bandwidth pct** *percentage* [**cbs-ratio** *ratio*]，CBS = 接口可用带宽×*percentage*×*ratio*÷100÷1000。
- 对于设置绝对值形式 **queue ef bandwidth** *bandwidth* [**cbs** *burst*]，CBS = *burst*，若不指定 *burst*，则 CBS = *bandwidth*×25。

相关配置可参考命令 **qos policy**、**traffic behavior** 和 **classifier behavior**。

【举例】

配置报文进入优先级队列，最大带宽为 200kbps，*burst* 为 5000bytes。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue ef bandwidth 200 cbs 5000
```

4.5.6 queue wfq

【命令】

queue wfq [**queue-number** *total-queue-number*]

undo queue wfq

【视图】

流行为视图

【缺省级别】

2：系统级

【参数】

queue-number *total-queue-number*：公平队列的数目，可取的值为 16、32、64、128、256、512、1024、2048、4096，即 2 的幂数，缺省为 256。

【描述】

queue wfq 命令用来为缺省类配置采用公平队列。**undo queue wfq** 命令用来取消配置。

配置了该命令的行为仅仅可以与缺省类关联使用，另外，该命令还可以搭配 **queue-length** 命令或 **wred** 命令使用。

相关配置可参考命令 **qos policy**、**traffic behavior** 和 **classifier behavior**。

【举例】

为缺省类配置使用 WFQ，队列数为 16。

```
<Sysname> system-view
[Sysname] traffic behavior test
[Sysname-behaviro-test] queue wfq queue-number 16
[Sysname] qos policy user1
[Sysname-qospolicy-user1] classifier default-class behavior test
```

4.5.7 queue-length

【命令】

queue-length *queue-length*

undo queue-length *queue-length*

【视图】

流行为视图

【缺省级别】

2：系统级

【参数】

queue-length：队列最大阈值，取值范围为 1～512。

【描述】

queue-length 命令用来配置最大队列长度，丢弃方式为尾部丢弃。**undo queue-length** 命令用来取消该配置。

缺省情况下，丢弃方式为尾部丢弃方式，队列长度为 64。

该命令必须在配置了 **queue af** 或 **queue wfq** 后使用。

配置 **queue-length** 后，若执行 **undo queue af** 和 **undo queue wfq** 命令，则 **queue-length** 也同时被取消，反之亦然。

配置 **queue-length** 后，若用 **wred** 命令配置为随机丢弃方式，则 **queue-length** 被取消，反之亦然。

相关配置可参考命令 **qos policy**、**traffic behavior** 和 **classifier behavior**。

【举例】

配置尾部丢弃，队列长度最大为 16。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue af bandwidth 200
[Sysname-behavior-database] queue-length 16
```

4.5.8 wred

【命令】

wred [**dscp** | **ip-precedence**]

undo wred

【视图】

流行为视图

【缺省级别】

2：系统级

【参数】

dscp：表明在为一个包计算丢弃概率时使用的是 DSCP 值。

ip-precedence：表明在为一个包计算丢弃概率时使用的是 IP 优先级值，缺省情况下使用的是 **ip-precedence**。

【描述】

wred 命令用来配置丢弃方式为加权随机早期检测。**undo wred** 命令用来取消该配置。

该命令必须在配置了 **queue af** 或 **queue wfq** 后使用。**wred** 和 **queue-length** 这两个命令不能同时有效。取消该配置时将删除 WRED 相关的其他配置。当接口上应用了配置 WRED 的策略后，原有的接口级的 WRED 配置失效。

相关配置可参考命令 **qos policy**、**traffic behavior** 和 **classifier behavior**。

【举例】

配置采用加权早期检测方式，丢弃概率以 IP 优先级计算。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue wfq
[Sysname-behavior-database] wred
```

4.5.9 wred dscp

【命令】

wred dscp *dscp-value* **low-limit** *low-limit* **high-limit** *high-limit* [**discard-probability** *discard-prob*]

undo wred dscp *dscp-value*

【视图】

流行为视图

【缺省级别】

2：系统级

【参数】

dscp-value：DSCP值，取值范围为 0～63，也可以是关键字，如 表 1-4 所示。

low-limit *low-limit*：WRED 下限。取值范围是 1～1024。

high-limit *high-limit*：WRED 上限。取值范围是 1～1024。

discard-probability *discard-prob*：丢弃概率。取值范围是 1～255，表示丢弃概率的分母。

【描述】

wred dscp 命令用来设置 WRED 各 DSCP 的下限、上限和丢弃概率。**undo wred dscp** 命令用来取消该配置。

进行本命令配置以前，必须已用 **wred dscp** 命令使能了基于 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。

相关配置可参考命令 **qos policy**、**traffic behavior** 和 **classifier behavior**。

【举例】

设置 DSCP 为 3 的报文的队列下限为 20，上限为 40，丢弃概率为 15。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue wfq
[Sysname-behavior-database] wred dscp
[Sysname-behavior-database] wred dscp 3 low-limit 20 high-limit 40 discard-probability 15
```

4.5.10 wred ip-precedence

【命令】

wred ip-precedence *precedence* **low-limit** *low-limit* **high-limit** *high-limit* [**discard-probability** *discard-prob*]

undo wred ip-precedence *precedence*

【视图】

流行为视图

【缺省级别】

2：系统级

【参数】

precedence：IP 优先级，取值范围为 0～7。

low-limit *low-limit*：WRED 下限。取值范围是 1～1024。

high-limit *high-limit*：WRED 上限。取值范围是 1～1024。

discard-probability *discard-prob*：丢弃概率。取值范围是 1～255，表示丢弃概率的分母。

【描述】

wred ip-precedence 命令用来设置 WRED 各优先级的下限、上限和丢弃概率。**undo wred ip-precedence** 命令用来取消配置。

进行本命令配置以前，必须已用 **wred** 命令使能了基于 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。

相关配置可参考命令 **qos policy**、**traffic behavior** 和 **classifier behavior**。

【举例】

设置优先级为 3 的报文的队列下限为 20，上限为 40，丢弃概率为 15。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue wfq
[Sysname-behaviro-database] wred ip-precedence
[Sysname-behavior-database] wred ip-precedence 3 low-limit 20 high-limit 40
discard-probability 15
```

4.5.11 wred weighting-constant

【命令】

wred weighting-constant *exponent*

undo wred weighting-constant

【视图】

流行为视图

【缺省级别】

2：系统级

【参数】

exponent：指数，取值范围为 1～16，缺省值为 9。

【描述】

wred weighting-constant 命令用来设置 WRED 计算平均队列长度的指数。**undo wred weighting-constant** 命令用来取消配置。

需配置了 **queue af** 或 **queue wfq**，并已用 **wred** 使能了 WRED 丢弃方式。

如果取消 **wred** 配置，**wred weighting-constant** 配置同时被取消。

相关配置可参考命令 **qos policy**、**traffic behavior** 和 **classifier behavior**。

【举例】

配置计算平均队列长度的指数为 6。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue af bandwidth 200
[Sysname-behavior-database] wred ip-precedence
[Sysname-behavior-database] wred weighting-constant 6
```

4.6 实时传输协议队列的配置命令

4.6.1 display qos rtpq interface

【命令】

display qos rtpq interface [*interface-type interface-number* [**pvc** { *pvc-name* [*vpi/vci*] | *vpi/vci* }]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

interface-type interface-number：指定的接口类型和接口编号。

pvc { *pvc-name* [*vpi/vci*] | *vpi/vci* }：只用于 ATM 接口，即可显示指定 ATM 接口上的指定 PVC 的信息。*pvc-name* 表示 PVC 名。*vpi/vci* 表示 VPI/VCI 值。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display qos rtpq interface 命令用来显示指定接口、指定 PVC 或所有接口及 PVC 的当前 IP RTP Priority 的队列信息，包括当前的 RTP 长度和 RTP 报文的丢包数。

如果不指定接口或 PVC，本命令将显示所有接口及 PVC 的 RTP 队列配置情况和统计信息。

如指定接口为 Virtual-Template 接口，将显示继承该 Virtual-Template 接口的所有 Virtual-Access 接口下的 QoS RTP 队列的信息，Virtual-Template 本身无 QoS 信息显示。

【举例】

显示当前 IP RTP Priority 的队列信息。

```
<Sysname> display qos rtpq interface
Interface: Ethernet1/1
Output queue : (RTP queuing: Size/Max/Outputs/Discards)  0/0/0/0
```

表4-7 display qos rtpq 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号结合在一起组成
Output queue	当前的输出队列
Size	队列中数据包数目
Max	队列中数据包的历史最大数目
Outputs	发送出去的数据包数目
Discards	丢弃的数据包数目

4.6.2 qos rtpq

【命令】

qos rtpq start-port *first-rtp-port-numbe*r **end-port** *last-rtp-port-number* **bandwidth** *bandwidth* [**cbs** *burst*]

undo qos rtpq

【视图】

接口视图/PVC 视图

【缺省级别】

2：系统级

【参数】

start-port *first-rtp-port-numbe*r：指定发起 RTP 报文的第一个 UDP 端口号，取值范围为 2000～65535。

end-port *last-rtp-port-number*：指定发起 RTP 报文的最后一个 UDP 端口号，取值范围为 2000～65535。

bandwidth *bandwidth*：RTP 队列所占用的带宽，取值范围为 8～1000000，单位为 kbps。

cbs *burst*：指定承诺突发尺寸，单位为字节，取值范围为 1500～2000000 字节。

【描述】

qos rtpq 命令用来启动接口或 PVC 下 RTP 队列特性，为某个 UDP 目的端口范围的 RTP 报文保留一个实时业务。**undo qos rtpq** 命令用来关闭接口或 PVC 的 RTP 队列特性。

缺省情况下，接口或 PVC 上不启动 RTP 队列特性。

该命令主要应用于对时延敏感的应用，如实时语音传输。**qos rtpq** 命令为语音业务提供最优先服务。

在配置 *bandwidth* 参数时，通常应该将其设置为比此实时业务所需的带宽总量要大一些，以预防突发流量的冲击。

注意

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 功能以保证队列生效。

【举例】

在接口 Serial2/0 上启动 RTP 队列特性，发起 RTP 报文的第一个 UDP 端口号为 16384，发起 RTP 报文的最后一个 UDP 端口号为 32767，RTP 报文占用 64kbps 的带宽，如果输出接口拥塞，进入 RTP 队列。

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] qos rtpq start-port 16384 end-port 32767 bandwidth 64
```

4.7 QoS令牌配置命令

4.7.1 qos qmtoken

【命令】

qos qmtoken *token-number*

undo qos qmtoken

【视图】

接口视图

【缺省级别】

2：系统级

【参数】

token-number：发送令牌数量，取值范围为 1～50。

【描述】

qos qmtoken 命令用来配置 QoS 的发送令牌数。**undo qos qmtoken** 命令用来取消 QoS 的发送令牌功能。

缺省情况下，设备上不启用此功能。

当进行 FTP 传输等工作时，由于上层协议提供了流控功能，可能会导致 QoS 的队列失效。QoS 的发送令牌功能提供了一种底层队列的流量控制机制，它可以根据令牌的数量控制向底层接口队列发送的报文数量。

通常，在进行 FTP 传输时，建议将接口的发送令牌数量设置为 1。

说明

- 在配置了此命令后，需要用 **shutdown/undo shutdown** 命令将接口重新启动，才能使能 QoS 的发送令牌功能。
- 目前只有串口、BRI 接口支持该命令。

【举例】

设置 QoS 的发送令牌数量为 1。

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] qos qmtoken 1
[Sysname-Serial2/0] shutdown
[Sysname-Serial2/0] undo shutdown
```

4.8 报文信息预提取命令

4.8.1 qos pre-classify

【命令】

qos pre-classify

undo qos pre-classify

【视图】

Tunnel 接口视图

【缺省级别】

2：系统级

【参数】

无

【描述】

qos pre-classify 命令用来使能 Tunnel 接口的报文信息预提取功能。**undo qos pre-classify** 命令用来关闭 Tunnel 接口的报文信息预提取功能。

缺省情况下，Tunnel 接口的报文信息预提取功能处于关闭状态。

【举例】

在 Tunnel 接口上使能报文信息预提取功能。

```
<Sysname> system-view
[Sysname] interface tunnel 1
[Sysname-Tunnel1] qos pre-classify
```

4.9 QoS分片报文预丢弃命令

4.9.1 qos fragment pre-drop

【命令】

qos fragment pre-drop

undo qos fragment pre-drop

【视图】

接口视图

【缺省级别】

2：系统级

【参数】

无

【描述】

qos fragment pre-drop 命令用来使能接口的本机分片预丢弃功能。**undo qos fragment pre-drop** 命令用来关闭接口的本机分片预丢弃功能。

缺省情况下，本机分片预丢弃功能处于关闭状态。

需要注意的是：

- 如果本机分片首片报文被丢弃，则后续分片报文都将被丢弃。
- 本机分片预丢弃功能可应用于 IPv4 和 IPv6 的本机分片报文。

【举例】

在接口 Ethernet1/1 上使能本机分片预丢弃功能。

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] qos fragment pre-drop
```

5 拥塞避免

5.1 WRED配置命令

5.1.1 display qos wred interface

【命令】

display qos wred interface [*interface-type interface-number* [**pvc** { *pvc-name* [*vpi/vci*] | *vpi/vci* }]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

interface-type interface-number：指定的接口类型和接口编号。

pvc { *pvc-name* [*vpi/vci*] | *vpi/vci* }：只用于 ATM 接口，即可显示指定 ATM 接口上的指定 PVC 的信息。*pvc-name* 表示 PVC 名。*vpi/vci* 表示 VPI/VCI 值。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display qos wred interface 命令用来显示指定接口、指定 PVC 或所有接口及 PVC 的 WRED 配置情况和统计信息。

如果不指定接口或 PVC，本命令将显示所有接口及 PVC 的 WRED 配置情况和统计信息。

【举例】

显示指定接口的 WRED 配置情况和统计信息。

```
<Sysname> display qos wred interface ethernet 1/1
Interface: Ethernet1/1
 Current WRED configuration:
 Exponent: 9 (1/512)
 Precedence Low     High    Discard      Random      Tail
            Limit   Limit   Probability  Discard     Discard
 ------------------------------------------------------------
 0          10      30      10           0           0
 1          100     1000    1            0           0
```

```
2           10          30          10          0           0
3           10          30          10          0           0
4           10          30          10          0           0
5           10          30          10          0           0
6           10          30          10          0           0
7           10          30          10          0           0
```

表5-1 display qos wred interface 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号结合在一起组成
Exponent	计算平均队列长度的指数
Precedence	报文的IP优先级
Random discard	随机丢弃的报文的数目
Tail discard	尾丢弃报文的数目
Low limit	队列下限
High limit	队列上限
Discard probability	计算丢弃概率时的分母

5.1.2 qos wred enable

【命令】

qos wred [**dscp** | **ip-precedence**] **enable**

undo qos wred enable

【视图】

接口视图/PVC 视图

【缺省级别】

2：系统级

【参数】

dscp：表明计算丢弃概率时使用的是 DSCP 值。

ip-precedence：表明计算丢弃概率时使用的是 IP 优先级值，缺省情况下使用的是 **ip-precedence**。

【描述】

qos wred enable 命令用来在接口或 PVC 上使能 WRED。**undo qos wred enable** 命令用来恢复缺省的队列丢弃方法。

缺省情况下，队列丢弃方法为尾丢弃。

注意

qos wred enable 命令在硬件口可直接配置，在软件口需要先在接口上应用 WFQ 队列。

相关配置可参考命令 **qos wfq** 和 **display qos wred interface**。

【举例】

在 Ethernet1/1 接口上使能 WRED，丢弃概率以 IP 优先级计算。

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] qos wfq queue-length 100 queue-number 512
[Sysname-Ethernet1/1] qos wred ip-precedence enable
```

5.1.3 qos wred dscp

【命令】

qos wred dscp *dscp-value* **low-limit** *low-limit* **high-limit** *high-limit* **discard-probability** *discard-prob*

undo qos wred dscp *dscp-value*

【视图】

接口视图/PVC 视图

【缺省级别】

2：系统级

【参数】

dscp-value：DSCP值，取值范围为 0～63，也可以是关键字，如 表 1-4 所示。

low-limit *low-limit*：WRED 下限。取值范围是 1～1024。

high-limit *high-limit*：WRED 上限。取值范围是 1～1024。

discard-probability *discard-prob*：丢弃概率。取值范围是 1～255，表示丢弃概率的分母。

【描述】

qos wred dscp 命令用来设置各 DSCP 优先级的下限、上限和丢弃概率。**undo qos wred dscp** 命令用来恢复缺省情况。

必须先使用 **qos wred dscp enable** 在接口或 PVC 上应用基于 DSCP 的 WRED 后，才可以进行本配置。阈值限制的是平均队列长度。

相关配置可参考命令 **qos wred enable** 和 **display qos wred interface**。

【举例】

在接口上设置 DSCP 优先级为 63 的报文的队列下限为 20，上限为 40，丢弃概率为 15。

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] qos wfq queue-length 100 queue-number 512
[Sysname-Ethernet1/1] qos wred dscp enable
[Sysname-Ethernet1/1] qos wred dscp 63 low-limit 20 high-limit 40 discard-probability 15
```

5.1.4 qos wred ip-precedence

【命令】

qos wred ip-precedence *ip-precedence* **low-limit** *low-limit* **high-limit** *high-limit* **discard-probability** *discard-prob*

undo qos wred ip-precedence *ip-precedence*

【视图】

接口视图/PVC 视图

【缺省级别】

2：系统级

【参数】

ip-precedence *ip-precedence*：IP 优先级，取值范围为 0～7。

low-limit *low-limit*：WRED 下限。取值范围是 1～1024。

high-limit *high-limit*：WRED 上限。取值范围是 1～1024。

discard-probability *discard-prob*：丢弃概率。取值范围是 1～255，表示丢弃概率的分母。

【描述】

qos wred ip-precedence 命令用来设置 IP 优先级的下限、上限和丢弃概率。**undo qos wred ip-precedence** 命令用来恢复缺省情况。

必须先使用 **qos wred enable** 在接口或 PVC 上应用基于 IP 优先级的 WRED 后，才可以进行本配置。阈值限制的是平均队列长度。

相关配置可参考命令 **qos wred enable** 和 **display qos wred interface**。

【举例】

在接口上设置 IP 优先级为 3 的报文的队列下限为 20，上限为 40，丢弃概率为 15。

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] qos wfq queue-length 100 queue-number 512
[Sysname-Ethernet1/1] qos wred ip-precedence enable
[Sysname-Ethernet1/1] qos wred ip-precedence 3 low-limit 20 high-limit 40
discard-probability 15
```

5.1.5 qos wred weighting-constant

【命令】

qos wred weighting-constant *exponent*

undo qos wred weighting-constant

【视图】

接口视图/PVC 视图

【缺省级别】

2：系统级

【参数】

weighting-constant *exponent*：计算平均队列长度的指数，取值范围为 1～16，缺省值为 9。

【描述】

qos wred weighting-constant 命令用来设置 WRED 计算平均队列长度的指数。**undo qos wred weighting-constant** 命令用来恢复缺省情况。

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

相关配置可参考命令 **qos wred enable** 和 **display qos wred interface**。

【举例】

在 Ethernet1/1 接口上配置计算平均队列长度的指数为 6。

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] qos wfq queue-length 100 queue-number 512
[Sysname-Ethernet1/1] qos wred enable
[Sysname-Ethernet1/1] qos wred weighting-constant 6
```

5.2 WRED表配置命令

5.2.1 display qos wred table

【命令】

display qos wred table [*table-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

table-name：要显示的 WRED 表的名字。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display qos wred table 命令用来显示 WRED 表的配置情况。

如果不指定表名字，本命令将显示所有 WRED 表配置情况。

【举例】

显示 WRED 表 1 的配置情况，表 1 是一个已经配置好的 WRED 参数表。

```
<Sysname> display qos wred table 1
```

```
Table Name: 1
Table Type: Queue based WRED
QID:  gmin  gmax  gprob  ymin  ymax  yprob  rmin  rmax  rprob  exponent
------------------------------------------------------------------------
 0    76    134     1    33     66     2    11     23     3      9
 1    76    134     1    33     66     2    11     23     3      9
 2    76    134     1    33     66     2    11     23     3      9
 3    76    134     1    33     66     2    11     23     3      9
 4    76    134     1    33     66     2    11     23     3      9
 5    76    134     1    33     66     2    11     23     3      9
 6    76    134     1    33     66     2    11     23     3      9
 7    76    134     1    33     66     2    11     23     3      9
```

表5-2 display qos wred table 命令显示信息描述表

字段	描述
Table name	WRED表名
Table type	WRED表类型
QID	队列ID
gmin	绿色报文的队列下限
gmax	绿色报文的队列上限
gprob	绿色报文的丢弃概率
ymin	黄色报文的队列下限
ymax	黄色报文的队列上限
yprob	黄色报文的丢弃概率
rmin	红色报文的队列下限
rmax	红色报文的队列上限
rprob	红色报文的丢弃概率
exponent	计算平均队列长度指数

5.2.2 qos wred table

【命令】

qos wred queue table *table-name*

undo qos wred table *table-name*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

queue：基于队列的表，拥塞时根据报文所在队列进行随机丢弃。

table *table-name*：指定表的名字。

【描述】

qos wred table 命令用来创建 WRED 表，同时进入该 WRED 表视图。**undo qos wred table** 命令用来删除全局 WRED 表。

缺省情况下，没有全局 WRED 表存在。

设备不允许删除正在使用的表。

基于队列的 WRED 表只能在二层端口上应用。二层端口上也只能应用基于队列的表。

相关配置可参考命令 **qos wfq**、**qos wred enable** 和 **display qos wred interface**。

【举例】

创建基于队列的 WRED 表 queue-table1。

```
<Sysname> system-view
[Sysname] qos wred queue table queue-table1
[Sysname-wred-table-queue-table1]
```

5.2.3 queue

【命令】

queue *queue-value* **low-limit** *low-limit* [**discard-probability** *discard-prob*]

undo queue { *queue-value* | **all** }

【视图】

WRED 表视图

【缺省级别】

2：系统级

【参数】

queue-value：队列编号，只适用于二层端口。

low-limit *low-limit*：WRED 下限。取值范围是 1～128。

discard-probability *discard-prob*：丢弃概率。取值范围是 1～16，表示丢弃概率的分母。

【描述】

queue 命令用来编辑基于 queue 的 WRED 表的内容。**undo queue** 命令用来恢复 WRED 表的内容为缺省值。

缺省情况下，基于队列的 WRED 全局表有一套可用的缺省参数。

相关配置可参考命令 **qos wred table**。

【举例】

修改基于 queue 的全局 WRED 表 queue-table1 的队列 1 的丢弃概率。

```
<Sysname> system-view
[Sysname] qos wred queue table queue-table1
[Sysname-wred-table-queue-table1]
```

```
[Sysname-wred-table-queue-table1] queue 1 low-limit 10 discard-probability 15
[Sysname-wred-table-queue-table1]
```

5.2.4 qos wred apply

【命令】

qos wred apply *table-name*

undo qos wred apply

【视图】

接口视图/端口组视图

【缺省级别】

2：系统级

【参数】

table-name：WRED 全局表的名字。

【描述】

qos wred apply 命令用来在接口上应用 WRED 全局表。**undo qos wred apply** 命令用来恢复端口缺省的尾丢弃模式，它同时取消 WRED 表的应用。

缺省情况下，端口采用尾丢弃。

基于队列的表内容只能应用在二层端口上。二层端口上只能应用基于队列的 WRED 全局表。

在接口视图下执行该命令，则该配置只在当前端口生效；在端口组视图下执行该命令，则该配置将在端口组中的所有端口生效。

相关配置可参考命令 **display qos wred interface**、**display qos wred table** 和 **qos wred table**。

MSR 系列路由器各款型对于本节所描述的命令及参数的支持情况有所不同，详细差异信息如下：

型号	命令	描述
MSR 900	**qos wred apply**	不支持
MSR 930		不支持
MSR 20-1X		不支持
MSR 20		不支持
MSR 30		仅安装了MIM-16FSW、DMIM-24FSW二层以太网交换模块的路由器支持
MSR 50		仅安装了FIC-16FSW、DFIC-24FSW二层以太网交换模块的路由器支持
MSR 2600		不支持

【举例】

在二层端口上应用基于队列的表 queue-table1。

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
```

```
[Sysname-Ethernet1/1] qos wred apply queue-table1
```

6 DAR

6.1 DAR配置命令

6.1.1 dar enable

【命令】

dar enable

undo dar enable

【视图】

接口视图

【缺省级别】

2：系统级

【参数】

无

【描述】

dar enable 命令用来使能接口的 DAR 流量识别功能。**undo dar enable** 命令用来关闭接口的 DAR 流量识别功能。

缺省情况下，接口的 DAR 流量识别功能处于关闭状态。

【举例】

使能接口 Ethernet1/1 的 DAR 流量识别功能。

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] dar enable
```

6.1.2 dar max-session-count

【命令】

dar max-session-count *count*

undo dar max-session-count

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

count：DAR 可识别的最大连接数目。

【描述】

dar max-session-count 命令用来配置 DAR 可识别的最大连接数。**undo dar max-session-count** 命令用来恢复 DAR 可识别的最大连接数的缺省值。

当有大量的数据流经设备时，若 DAR 对其进行一一识别，将会消耗大量的系统资源，从而影响其它功能模块的正常工作。为了避免这种现象，用户可以对 DAR 能够识别的最大连接数目进行限制，以节省宝贵的系统资源。

- 对于 HTTP、FTP、RTP、RTCP 这些协议，DAR 是按照协议规则来识别，当连接数目超过设定的最大阈值时，DAR 将不再对到来的新连接的 TCP 和 UDP 报文进行识别，直接将其标记为无法识别报文。
- 对于其他 TCP/UDP 协议，DAR 是根据协议的端口号来识别，即使连接数目超过设定的最大阈值，仍然可以对报文进行识别。

【举例】

配置 DAR 可识别的最大连接数为 1000。

```
<Sysname> system-view
[Sysname] dar max-session-count 1000
```

6.1.3 dar p2p signature-file

【命令】

dar p2p signature-file *filename*

undo dar p2p signature-file

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

filename：P2P 特征文件名称，必须以“.mtd”为后缀。

【描述】

dar p2p signature-file 命令用来加载指定的 P2P 特征文件。**undo dar p2p signature-file** 命令用来卸载指定的 P2P 特征文件。

缺省情况下，系统没有加载 P2P 特征文件。

需要注意的是，系统只能加载根目录下的特征文件，请将要加载的特征文件放在根目录下。

【举例】

加载特征文件 p2p.mtd。

```
<Sysname> system-view
[Sysname] dar p2p signature-file flash:/p2p.mtd
```

6.1.4 dar protocol

【命令】

dar protocol *protocol-name* { **tcp** | **udp** } **port** { *port-value*&<1-16> | **range** *port-min port-max* } *

undo dar protocol *protocol-name* { **tcp** | **udp** } **port**

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

protocol-name：应用协议类型，取值范围包括 表 6-1 中列出的所有协议以及RTP、RTCP、user-defined01、user-defined02、……、user-defined10。初始状态的 10 个用户预定义协议（user-defined01～user-defined10）是没有指定端口号的，只有指定了端口号以后才会生效。同时，用户预定义协议也可以使用**dar protocol-rename**命令来更改名称。

tcp：基于 TCP 协议。

udp：基于 UDP 协议。

port-value：协议的端口号，取值范围为 1～65535，且不能与 DAR 特性中其他应用协议已设置的端口号冲突。&<1-16>表示前面的参数最多可以输入 16 次。每个协议最多可以设置 16 个端口号。

range *port-min port-max*：设置端口号的范围，*port-min* 表示范围内的最小端口号，*port-max* 表示范围内的最大端口号。最大端口号和最小端口号之间的差值要小于 1000，即 *port-max* – *port-min* < 1000。端口号范围内不能含有 DAR 特性中其他应用协议已设置的端口。

表6-1 协议的缺省端口号

协议名称	协议类型	缺省端口号
BGP	TCP/UDP	179
Cifs	TCP	445
Citrix	TCP	1494
Citrix	UDP	1604
CUSeeMe	TCP	7648、7649
CUSeeMe	UDP	7648、7649、24032
DHCP	UDP	67、68
DNS	TCP/UDP	53
Exchange	TCP	135
Fasttrack	TCP	1214
Finger	TCP	79
FTP	TCP	21
Gnutella	TCP	6346、6347、6348、6349、6355、5634
Gopher	TCP/UDP	70

协议名称	协议类型	缺省端口号
H323	TCP	1300、1718、1719、1720、11000～11999
H323	UDP	1300、1718、1719、1720、11720
HTTP	TCP	80
IMAP	TCP/UDP	143、220
IRC	TCP/UDP	194
Kerberos	TCP/UDP	88、749
L2TP	UDP	1701
LDAP	TCP/UDP	389
Mgcp	TCP	2427、2428、2727
Mgcp	UDP	2427、2727
Napster	TCP	6699、8875、8888、7777、6700、6666、6677、6688、4444、5555
NetBIOS	TCP	137、138、139
NetBIOS	UDP	137、138、139
Netshow	TCP	1755
NFS	TCP/UDP	2049
NNTP	TCP/UDP	119
Notes	TCP/UDP	1352
Novadign	TCP/UDP	3460、3461、3462、3463、3464、3465
NTP	TCP/UDP	123
PCAnywhere	TCP	5631、65301
PCAnywhere	UDP	22、5632
POP3	TCP/UDP	110
PPTP	TCP	1723
Printer	TCP/UDP	515
RCMD	TCP	512、513、514
RIP	UDP	520
RSVP	UDP	1698、1699
RTSP	TCP	554
Secure-FTP	TCP	990
Secure-HTTP	TCP	443
Secure-IMAP	TCP/UDP	585、993
Secure-IRC	TCP/UDP	994
Secure-LDAP	TCP/UDP	636

协议名称	协议类型	缺省端口号
Secure-NNTP	TCP/UDP	563
Secure-POP3	TCP/UDP	995
Secure-TELNET	TCP	992
SIP	TCP/ UDP	5060
Skinny	TCP	2000、2001、2002
SMTP	TCP	25
SNMP	TCP/UDP	161、162
SOCKS	TCP	1080
Sqlnet	TCP	1521
Sqlserver	TCP	1433
SSH	TCP	22
Streamwork	UDP	1558
Sunrpc	TCP/UDP	111
Syslog	UDP	514
Telnet	TCP	23
Tftp	UDP	69
Vdolive	TCP	7000
Winmx	TCP	6699
XWindows	TCP	6000、6001、6002、6003

【描述】

dar protocol 命令用来配置 DAR 应用协议的端口号。**undo dar protocol** 命令用来恢复 DAR 应用协议的端口号为缺省值。

缺省情况下，10 个用户预定义协议、RTP和RTCP协议无缺省端口号，其他各协议的缺省端口号如表 6-1 所示。

【举例】

配置 RTP 协议的端口号为 36000、36001 和 40000～40999。

```
<Sysname> system-view
[Sysname] dar protocol rtp udp port 36000 36001 range 40000 40999
```

6.1.5 dar protocol-group

【命令】

dar protocol-group *group-id*

undo dar protocol-group *group-id*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

protocol-id：协议组号，取值范围为 1～64。

【描述】

dar protocol-group 命令用来创建 P2P 协议组并进入协议组视图。**undo dar protocol-group** 命令用来删除指定的协议组。

缺省情况下，系统中不存在协议组。

【举例】

创建 P2P 协议组 1。

```
<Sysname> system-view
[Sysname] dar protocol-group 1
[Sysname-protocol-group-1]
```

6.1.6 dar protocol-rename

【命令】

dar protocol-rename *old-name user-defined-name*

undo dar protocol-rename *user-defined-name*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

old-name：用户预定义协议的初始名称，初始名称为 **user-defined01**、**user-defined02**、……、**user-defined10**。

user-defined-name：用户预定义协议的新名称，取值范围为 1～31 个字符。新的名称不能与已存在的协议名称冲突，而且不能为 all、total、tcp、udp、ip 或 user-defined01、user-defined02、……、user-defined10。

【描述】

dar protocol-rename 命令用来对用户预定义协议进行重命名。**undo dar protocol-rename** 命令用来恢复用户预定义协议的缺省名称。

缺省情况下，用户预定义协议的名称为 **user-defined01**、**user-defined02**、……、**user-defined10**。

【举例】

将用户预定义协议 user-defined01 的名称改为 hello。

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

```
[Sysname] dar protocol-rename user-defined01 hello
```

将用户预定义协议 user-defined01 的名称恢复为缺省名称。

```
<Sysname> system-view
[Sysname] undo dar protocol-rename hello
```

6.1.7 dar protocol-statistic

【命令】

dar protocol-statistic [**flow-interval** *time*]

undo dar protocol-statistic

【视图】

接口视图

【缺省级别】

2：系统级

【参数】

flow-interval *time*：统计的时间间隔，取值范围为 1～30，单位为分钟，缺省值为 5 分钟。

【描述】

dar protocol-statistic 命令用来使能 DAR 的报文统计功能。**undo dar protocol-statistic** 命令用来关闭 DAR 的报文统计功能。

缺省情况下，未使能 DAR 的报文统计功能。

通过使能 DAR 的报文统计功能，用户可以及时对各个接口上的应用协议的报文个数、数据流量、以及流量的历史平均速率和历史最大速率进行监控，便于对数据流实施相应的策略。

【举例】

使能接口 Ethernet1/1 的 DAR 的报文统计功能，并配置统计时间间隔为 7 分钟。

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] dar protocol-statistic flow-interval 7
```

6.1.8 display dar information

【命令】

display dar information [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display dar information 命令用来显示 DAR 特性模块的信息。

【举例】

显示 DAR 特性模块的信息。

```
<Sysname> display dar information
Max session count       : 65536
Watched session count   : 1000
```

表6-2 display dar information 命令显示信息描述表

字段	描述
Max session count	最大会话数目
Watched session count	已监视的会话数目

6.1.9 display dar protocol

【命令】

display dar protocol { *protocol-name* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

protocol-name：显示指定协议的信息，取值范围与 **dar protocol** 命令中 *protocol-name* 的取值范围相同。

all：显示所有协议的信息。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display dar protocol 命令用来显示 DAR 协议的相关信息。

对于静态端口协议和一般应用层协议，显示的是其 TCP/UDP 端口号。

【举例】

显示所有协议的信息。

```
<Sysname> display dar protocol all
Protocol         TCP/UDP  Port
---------------- -------- -----------
bgp              tcp      179
                 udp      179
cifs             tcp      445
citrix           tcp      1494
                 udp      1604
cuseeme          tcp      7648 7649
                 udp      7648 7649 24032
dhcp             udp      67 68
dns              tcp      53
                 udp      53
exchange         tcp      135
fasttrack        tcp      1214
finger           tcp      79
ftp              tcp      21
gnutella         tcp      5634 6355 range 6346 6349
gopher           tcp      70
                 udp      70
h323             tcp      1300 1718 1719 1720 range 11000 11999
                 udp      1300 1718 1719 1720 11720
http             tcp      80
imap             tcp      143 220
                 udp      143 220
irc              tcp      194
                 udp      194
kerberos         tcp      88 749
                 udp      88 749
l2tp             udp      1701
ldap             tcp      389
                 udp      389
mgcp             tcp      2427 2428 2727
                 udp      2427 2727
napster          tcp      6699 8875 8888 7777 6700 6666 6677 6688 4444 5555
netbios          tcp      137 138 139
                 udp      137 138 139
netshow          tcp      1755
nfs              tcp      2049
                 udp      2049
nntp             tcp      119
                 udp      119
notes            tcp      1352
                 udp      1352
novadign         tcp      3460 3461 3462 3463 3464 3465
                 udp      3460 3461 3462 3463 3464 3465
```

ntp	tcp	123
	udp	123
pcanywhere	tcp	5631 65301
	udp	22 5632
pop3	tcp	110
	udp	110
pptp	tcp	1723
printer	tcp	515
	udp	515
rcmd	tcp	512 513 514
rip	udp	520
rsvp	udp	1698 1699
rtcp		
rtp		
rtsp	tcp	554
secure-ftp	tcp	990
secure-http	tcp	443
secure-imap	tcp	585 993
	udp	585 993
secure-irc	tcp	994
	udp	994
secure-ldap	tcp	636
	udp	636
secure-nntp	tcp	563
	udp	563
secure-pop3	tcp	995
	udp	995
secure-telnet	tcp	992
sip	tcp	5060
	udp	5060
skinny	tcp	2000 2001 2002
smtp	tcp	25
snmp	tcp	161 162
	udp	161 162
socks	tcp	1080
sqlnet	tcp	1521
sqlserver	tcp	1433
ssh	tcp	22
streamwork	udp	1558
sunrpc	tcp	111
	udp	111
syslog	udp	514
telnet	tcp	23
tftp	udp	69
user-defined01		
user-defined02		
user-defined03		
user-defined04		

```
user-defined05
user-defined06
user-defined07
user-defined08
user-defined09
user-defined10
vdolive         tcp       7000
winmx           tcp       6699
xwindows        tcp       range 6000 6003
```

表6-3 display dar protocol 命令显示信息描述表

字段	描述
Protocol	协议名
TCP/UDP	基于TCP还是基于UDP
Port	端口号

6.1.10 display dar protocol-rename

【命令】

display dar protocol-rename [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display dar protocol-rename 命令用来显示用户预定义协议的重命名信息。

【举例】

显示用户预定义协议的重命名信息。

```
<Sysname> display dar protocol-rename
Default Name     User Defined Name
---------------- --------------------
user-defined01   merry
user-defined02
```

```
user-defined03
user-defined04
user-defined05
user-defined06
user-defined07
user-defined08
user-defined09
user-defined10
```

表6-4 display dar protocol-rename 命令显示信息描述表

字段	描述
Default Name	默认协议名
User Defined Name	用户定义协议名

6.1.11 display dar protocol-statistic

【命令】

display dar protocol-statistic [**p2p** | **protocol** *protocol-name* | **top** *top-number* | **all**] [**interface** *interface-type interface-number*] [**direction** { **in** | **out** }] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

p2p：查看 P2P 协议报文的统计信息。

protocol *protocol-name*：查看指定的协议，*protocol-name* 的取值范围与 **if-match protocol** 中 **protocol** 关键字后可输入的参数范围相同。

top *top-number*：查看流量最大的 *top-number* 个协议，取值范围为 1～16。

all：查看所有协议报文的统计信息。

interface-type interface-number：指定查看的接口类型及接口编号。

direction：指定查看的流量的方向，缺省为双向。

in：查看入方向的流量。

out：查看出方向的流量。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display dar protocol-statistic 命令用来显示 DAR 的报文统计信息。

【举例】

显示接口 Ethernet1/1 的所有协议报文的统计信息。

```
<Sysname> display dar protocol-statistic interface ethernet 1/1
Interface: Ethernet1/1
Protocol       In/Out  Packet Count    Byte Count        Bit Rate  Max Bit Rate
                                                         in  5 min  in  5 min
                                                         (bps)     (bps)
-------- ------ ------------ -------------- ------------ -----------
netbios        IN      5               692              0         0
tcp-handshake  IN      1               48               0         0
               OUT     2               88               0         0
unknown-tcp    IN      1               42               0         0
Total          IN      7               782              0         0
               OUT     5               214              0         0
```

显示接口 Ethernet1/1 的 P2P 协议报文的统计信息。

```
<Sysname> display dar protocol-statistic p2p interface ethernet 1/1
Interface: Ethernet1/1
Protocol       In/Out  Packet Count    Byte Count        Bit Rate  Max Bit Rate
                                                         in  5 min  in  5 min
                                                         (bps)     (bps)
MSN            IN      0               0                0         0
               OUT     0               0                0         0
Yahoo Message  IN      0               0                0         0
               OUT     0               0                0         0
Total          IN      0               0                0         0
               OUT     3               126              0         0
```

表6-5 display dar protocol-statistic 命令显示信息描述表

字段	描述
Protocol	协议名
In/Out	报文的方向（入/出）
Packet Count	报文数
Byte Count	字节数
Bit Rate in 5 min(bps)	5分钟内的比特率，单位为bps
Max Bit Rate in 5 min(bps)	5分钟内的最大比特率，单位为bps

6.1.12 if-match protocol

【命令】

if-match [**not**] **protocol** *protocol-name*

undo if-match [**not**] **protocol** *protocol-name*

【视图】

类视图

【缺省级别】

2：系统级

【参数】

not：指定本规则为不匹配指定匹配规则的规则。

protocol-name：匹配协议的名称，取值范围为 **bgp**、**cifs**、**citrix**、**cuseeme**、**dhcp**、**dns**、**egp**、**eigrp**、**exchange**、**fasttrack**、**finger**、**ftp**、**gnutella**、**gopher**、**gre**、**h323**、**icmp**、**igmp**、**imap**、**ip**、**ipinip**、**ipsec**、**ipv6**、**irc**、**kerberos**、**l2tp**、**ldap**、**mgcp**、**napster**、**netbios**、**netshow**、**nfs**、**nntp**、**notes**、**novadign**、**ntp**、**pcanywhere**、**pop3**、**pptp**、**printer**、**rcmd**、**rip**、**rsvp**、**rtcp**、**rtsp**、**secure-ftp**、**secure-http**、**secure-imap**、**secure-irc**、**secure-ldap**、**secure-nntp**、**secure-pop3**、**secure-telnet**、**sip**、**skinny**、**smtp**、**snmp**、**socks**、**sqlnet**、**sqlserver**、**ssh**、**streamwork**、**sunrpc** 、**syslog**、**telnet**、**tftp**、**vdolive**、**winmx**、**xwindows**、**unknown-tcp**、**unknown-udp**、**unknown-others**、**user-defined01**、**user-defined02**……**user-defined10**（如果 **user-defined01**～**user-defined10** 被改了名字，则为修改后的名字）中的一个。其中 **unknown-tcp** 为不可识别的 TCP 协议报文，**unknown-udp** 为不可识别的 UDP 协议报文，**unknown-others** 为不可识别的其它 IP 协议报文。**user-defined01**、**user-defined02**……**user-defined10** 为用户预定义协议报文，在没有使用 **dar protocol** 命令为其分配端口号前是无效的。

【描述】

if-match protocol 命令用来定义协议匹配规则。**undo if-match protocol** 命令用来删除协议匹配规则。

缺省情况下，未配置协议匹配规则。

【举例】

定义类 smtp-class，配置匹配规则匹配 SMTP 协议。

```
<Sysname> system-view
[Sysname] traffic classifier smtp-class
[Sysname-classifier-smtp-class] if-match protocol smtp
```

6.1.13 if-match protocol http

【命令】

if-match [**not**] **protocol http** [**url** *url-string* | **host** *hostname-string* | **mime** *mime-type*]

undo if-match [**not**] **protocol http** [**url** *url-string* | **host** *hostname-string* | **mime** *mime-type*]

【视图】

类视图

【缺省级别】

2：系统级

【参数】

not：指定本规则为不匹配指定匹配规则的规则。

url：根据 HTTP 报文中的 URL 进行匹配。

url-string：在 HTTP 报文中进行匹配的 URL，取值范围为 1～32 个字符，表示 HTTP 报文 URL 中包含 *url-string* 所包含的字符串，支持简单通配符匹配。

host：根据 HTTP 报文中的 host name 进行匹配。

hostname-string：HTTP 报文中进行匹配的 host name，取值范围为 1～32 个字符，表示 HTTP 报文 host name 中包含 *hostname-string* 所包含的字符串，支持简单通配符匹配。

mime：根据 HTTP 报文中的 MIME 类型进行匹配。

mime-type：在 HTTP 报文中进行匹配的 MIME 类型，取值范围为 1～32 个字符，表示 HTTP 报文 MIME 类型中包含 *mime-type* 所包含的字符串，支持简单通配符匹配。

说明

简单通配符匹配规则如 表 6-6 所示。

表6-6 简单通配符匹配规则

符号	含义
*	匹配0个或任意多个字符，字符包括数字、大小写字母、连字符、下划线
#	匹配一个字符，字符包括数字、大小写字母、连字符、下划线
|	匹配左右两边任意一边的字符串
(|)	在一个范围内匹配左右两边任意一边的字符串。例如，“index.(htm|jsp)”的含义为：既匹配“index.htm”又匹配“index.jsp”
[ ]	匹配在方括号中指定的任意一个字符，或匹配一个特殊字符，特殊字符包括*、#、[、(、|、)。例如，“[0-9]”代表所有的数字，“[*]”代表“*”这个字符，“[[]”代表“[”这个字符

【描述】

if-match protocol http 命令用来配置 HTTP 协议的匹配规则。**undo if-match protocol http** 命令用来删除 HTTP 协议的匹配规则。

缺省情况下，未配置 HTTP 协议的匹配规则。

【举例】

定义类 http-class，配置匹配规则为 host name 为*.abc.com 的 HTTP 报文。

```
<Sysname> system-view
[Sysname] traffic classifier http-class
[Sysname-classifier-http-class] if-match protocol http host *.abc.com
```

6.1.14 if-match protocol rtp

【命令】

if-match [**not**] **protocol rtp** [**payload-type** { **audio** | **video** | *payload-string* &<1-16> } *]

undo if-match [**not**] **protocol rtp** [**payload-type** { **audio** | **video** | *payload-string*&<1-16> } *]

【视图】

类视图

【缺省级别】

2：系统级

【参数】

not：指定本规则为不匹配指定匹配规则的规则。

payload-type：对载荷类型进行匹配。

audio：对音频 RTP 载荷类型进行匹配。

video：对视频 RTP 载荷类型进行匹配。

payload-string：在 RTP 报文中进行匹配的载荷类型，取值范围为 0～127。&<1-16>表示前面的参数最多可以输入 16 次。

【描述】

if-match protocol rtp 命令用来配置 RTP 协议的匹配规则。**undo if-match protocol rtp** 命令用来删除 RTP 协议的匹配规则。

若不指定载荷类型，表示匹配所有 RTP 报文。

缺省情况下，未配置 RTP 协议的匹配规则。

【举例】

定义类 rtp-class1，配置匹配规则为匹配载荷类型为视频的 RTP 报文。

```
<Sysname> system-view
[Sysname] traffic classifier rtp-class1
[Sysname-classifier-rtp-class1] if-match protocol rtp payload-type video
```

定义类 rtp-class2，配置匹配规则为匹配载荷类型为 0、1、4、5、6、10 或 64 的 RTP 报文。

```
<Sysname> system-view
[Sysname] traffic classifier rtp-class2
[Sysname-classifier-rtp-class2] if-match protocol rtp payload-type 0 1 4 5 6 10 64
```

6.1.15 protocol

【命令】

protocol *protocol-name*

undo protocol *protocol-name*

【视图】

协议组视图

【缺省级别】

2：系统级

【参数】

protocol-name：协议名称，为 1～31 个字符的字符串。

【描述】

protocol 命令用来向当前协议组中添加协议。**undo protocol** 命令用来从当前协议组中删除协议。

缺省情况下，协议组中没有任何协议。

需要注意的是，只有特征文件中包含的协议才能加入协议组中。对于已经添加到协议组中的协议，如果在新加载的特征文件中不包含该协议，则该协议在特征文件加载时自动从协议组中删除。

【举例】

向协议组 1 中添加 MSN 协议。

```
<Sysname> system-view
[Sysname] dar protocol-group 1
[Sysname-protocol-group-1] protocol msn
```

6.1.16 reset dar protocol-statistic

【命令】

reset dar protocol-statistic { { { **p2p** | **protocol** *protocol-name* } | **interface** *interface-type interface-number* } * | **all** }

【视图】

用户视图

【缺省级别】

1：监控级

【参数】

p2p：清除 P2P 协议的统计信息。

protocol *protocol-name*：清除指定协议的统计信息，*protocol-name* 的取值范围与 **if-match protocol** 中 **protocol** 关键字后可输入的参数范围相同。

interface-type interface-number：指定接口类型和接口编号。

all：清除所有协议的统计信息。

【描述】

reset dar protocol-statistic 命令用来清除 DAR 的协议统计信息，即将统计的结果重置为 0。

【举例】

清除接口 Ethernet1/1 的 FTP 协议的统计。

```
<Sysname> reset dar protocol-statistic protocol ftp interface ethernet 1/1
```

清除所有协议的统计信息。

```
<Sysname> reset dar protocol-statistic all
```

6.1.17 reset dar session

【命令】

reset dar session

【视图】

用户视图

【缺省级别】

2：系统级

【参数】

无

【描述】

reset dar session 命令用来清除所有的会话连接缓存信息。

【举例】

清除会话连接缓存信息。

```
<Sysname> reset dar session
```

目 录

1 帧中继QoS

1.1 帧中继QoS配置命令

1.1.1 apply policy outbound

【命令】

apply policy *policy-name* **outbound**

undo apply policy outbound

【视图】

帧中继类视图

【缺省级别】

2：系统级

【参数】

policy-name：应用的策略名称，为 1～31 个字符的字符串。

【描述】

apply policy outbound 命令用来应用 QoS 策略。**undo apply policy outbound** 命令用来取消应用的 QoS 策略。

【举例】

定义一个名为 class1 的类。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl 3101
[Sysname-classifier-class1] quit
```

定义一个名为 behavior1 的流行为。

```
[Sysname] traffic behavior behavior1
[Sysname-behavior-behavior1] queue af bandwidth 56
[Sysname-behavior-behavior1] quit
```

定义一个名为 policy1 的策略，并将类 class1 与行为 behavior1 关联。

```
[Sysname] qos policy policy1
[Sysname-qospolicy-policy1] classifier class1 behavior behavior1
[Sysname-qospolicy-policy1] quit
```

将已定义的策略应用到名为 test1 的帧中继类上。

```
[Sysname] fr class test1
[Sysname-fr-class-test1] apply policy policy1 outbound
```

1.1.2 cbs

【命令】

cbs [**inbound** | **outbound**] *committed-burst-size*

undo cbs [**inbound** | **outbound**]

【视图】

帧中继类视图

【缺省级别】

2：系统级

【参数】

inbound：报文入方向的承诺突发尺寸，本参数仅当接口使能帧中继流量监管时有效。

outbound：报文出方向的承诺突发尺寸，本参数仅当接口使能帧中继流量整形时有效。

committed-burst-size：承诺突发尺寸，取值范围为 300～16000000，单位为 bit，缺省值为 56000bits。

【描述】

cbs 命令用来配置帧中继虚电路的 CBS（Committed burst size，承诺突发尺寸）。**undo cbs** 命令用来恢复缺省值。

如果配置时不指定报文方向，则表示同时配置在入方向和出方向上。

承诺突发尺寸是帧中继网络在一个 Tc 的时间间隔内，承诺可以发送的报文流量。当网络没有发生拥塞时，帧中继网络保证这部分流量可以被成功发送。

相关配置可参考命令 **ebs**、**cir allow** 和 **cir**。

【举例】

配置名为 test1 的帧中继类在入方向和出方向上的 CBS 为 64000bits。

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] cbs 64000
```

1.1.3 cir

【命令】

cir *committed-information-rate*

undo cir

【视图】

帧中继类视图

【缺省级别】

2：系统级

【参数】

committed-information-rate：承诺信息速率，取值范围为 1000～45000000，单位为 bps，缺省值是 56000bps。

【描述】

cir 命令用来配置帧中继虚电路的 CIR（Committed Information Rate, 承诺信息速率）。**undo cir** 命令用来恢复缺省值。

CIR 是虚电路所能提供的最低发送速率，它保证了用户在网络拥塞时仍然能够以此速率发送数据。

当网络发生拥塞时，DCE 将向 DTE 发送 BECN 标志位为 1 的报文。DTE 接收到这个报文后，会将虚电路的发送速率由 CIR ALLOW 逐渐调低到 CIR；如果 DTE 在 125ms 内没有再收到 BECN 标志位为 1 的报文，它会将虚电路的发送速率恢复为 CIR ALLOW。

相关配置可参考命令 **cbs**、**ebs** 和 **cir allow**。

说明

配置时，承诺信息速率不能大于允许的承诺信息速率。

【举例】

配置名为 test1 的帧中继类的 CIR 为 32000bps。

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] cir 32000
```

1.1.4 cir allow

【命令】

cir allow [**inbound** | **outbound**] *committed-information-rate*

undo cir allow [**inbound** | **outbound**]

【视图】

帧中继类视图

【缺省级别】

2：系统级

【参数】

inbound：报文入方向所允许的承诺信息速率，本参数仅当接口使能帧中继流量监管时有效。

outbound：报文出方向所允许的承诺信息速率，本参数仅当接口使能帧中继流量整形时有效。

committed-information-rate：允许的承诺信息速率，取值范围为 1000～45000000，单位为 bps，缺省值为 56000bps。

【描述】

cir allow 命令用来配置帧中继虚电路允许的 CIR ALLOW（Committed Information Rate ALLOW，允许的承诺信息速率）。**undo cir allow** 命令用来恢复缺省值。

允许的承诺信息速率是正常情况下帧中继网络所能提供的发送速率，当网络没有发生拥塞时，它保证用户能够以此速率发送数据。

如果配置时不指定报文方向，则表示同时配置在入方向和出方向上。

相关配置可参考命令 **cbs**、**ebs** 和 **cir**。

说明

配置时，允许的承诺信息速率不能小于承诺信息速率。

【举例】

配置名为 test1 的帧中继类的 CIR ALLOW 为 64000bps。

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] cir allow 64000
```

1.1.5 congestion-threshold

【命令】

congestion-threshold { **de** | **ecn** } *queue-percentage*

undo congestion-threshold { **de** | **ecn** }

【视图】

帧中继类视图

【缺省级别】

2：系统级

【参数】

de：当拥塞发生时，丢弃 DE 标志位为 1 的帧中继报文。

ecn：当拥塞发生时，将帧中继报文的 BECN 和 FECN 标志位置 1。

queue-percentage：网络拥塞门限值，为虚电路队列的使用率，即虚电路当前队列长度占队列总长度的百分比，取值范围为 1～100，缺省值为 100。

【描述】

congestion-threshold 命令用来使能帧中继虚电路的拥塞管理功能。**undo congestion-threshold** 命令用来关闭此功能。

缺省情况下，帧中继虚电路的拥塞管理功能处于关闭状态。

当虚电路当前队列的长度占虚电路队列总长度的百分比超过配置的拥塞门限值时，认为虚电路上发生拥塞，开始对虚电路上的报文进行拥塞处理：丢弃 DE 标志位为 1 的帧中继报文或者将帧中继报文的 BECN 和 FECN 标志位置 1。

相关配置可参考命令 **fr congestion-threshold**。

【举例】

配置对于名为 test1 的帧中继类，当虚电路当前队列长度超过总长度的 80%时，开始丢弃 DE 标志位为 1 的帧中继报文。

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] congestion-threshold de 80
```

1.1.6 cq

【命令】

cq cql *cql-index*

undo cq

【视图】

帧中继类视图

【缺省级别】

2：系统级

【参数】

cql *cql-index*：定制队列的组号，取值范围为 1～16。

【描述】

cq 命令用来将帧中继虚电路的队列类型配置为 CQ（Custom Queuing，定制队列）。**undo cq** 命令用来将虚电路的队列类型恢复为 FIFO。

缺省情况下，虚电路的队列类型为 FIFO。

对同一个帧中继类重复使用本命令，将覆盖原来的配置。

相关配置可参考命令 **wfq**、**pq** 和 **fr pvc-pq**。

【举例】

将定制列表的第 10 组应用到名为 test1 的帧中继类上。

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] cq cql 10
```

1.1.7 display fr class-map

【命令】

display fr class-map { **fr-class** *class-name* | **interface** *interface-type interface-number* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

fr-class *class-name*：显示指定帧中继类与接口的映射关系。*class-name* 表示帧中继类名称，为 1～30 个字符的字符串。

interface *interface-type interface-number*：显示指定接口与帧中继类的映射关系。*interface-type interface-number* 用来指定接口类型与编号。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display fr class-map 命令用来显示帧中继类与接口（包括属于该接口的 DLCI、该接口下的子接口以及子接口下的 DLCI）的映射关系。

参数中可以指定帧中继类名称，也可以指定主接口，但是不可以指定子接口。

【举例】

显示接口 Serial2/0 与帧中继类的映射关系。

```
<Sysname> display fr class-map interface serial 2/0
Serial2/0
  fr-class ts1
  Serial2/0.1
    fr-class ts2
    fr dlci  100    Serial2/0
      fr-class ts
    fr dlci 222    Serial2/0.1
      fr-class ts
```

表1-1 **display fr class-map** 命令显示信息描述表

字段	描述
Serial2/0 fr-class ts1	帧中继接口及关联的帧中继类
Serial2/0.1 fr-class ts2	帧中继子接口及关联的帧中继类
fr dlci 100 Serial2/0 fr-class ts	帧中继接口下的虚电路及关联的帧中继类
fr dlci 222 Serial2/0.1 fr-class ts	帧中继子接口下的虚电路及关联的帧中继类

显示帧中继类 ts 与接口的映射关系。

```
<Sysname> display fr class-map fr-class ts
    fr dlci  100    Serial2/0
      fr-class ts
    fr dlci 222    Serial2/0.1
      fr-class ts
```

1.1.8 display fr fragment-info

【命令】

display fr fragment-info [**interface** *interface-type interface-number*] [*dlci-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

interface *interface-type interface-number*：显示指定接口的帧中继分片信息。*interface-type interface-number* 用来指定接口类型与编号。

dlci-number：显示指定 DLCI 的帧中继分片信息。*dlci-number* 表示 DLCI 编号，取值范围为 16～1007。指定该参数将显示详细信息。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display fr fragment-info 命令用来显示帧中继分片信息。

相关配置可参考命令 **fragment**。

【举例】

显示所有接口上的帧中继分片信息。

```
<Sysname> display fr fragment-info
interface Serial2/0:1:
dlci    type                size        in/out/drop
200     FRF12(End to End)   80           0/0/0
```

表1-2 **display fr fragment-info 命令显示信息描述表**

字段	描述
interface	所在接口
dlci	DLCI号
type	分片类型，包括三种：FRF.12、FRF.11 Annex C、Motorola fragment
size	分片大小，单位为字节
in/out/drop	接收/发送/丢弃的分片报文数

显示指定接口上的帧中继分片信息。

```
<Sysname> display fr fragment-info interface serial 2/0:1 200
Type : FRF12(End to End)
 Size : 80
Data-level: 200    Voice-level: 0
 Pre-fragment:
    out pkts : 0             out bytes :0
 Fragmented:
    in pkts : 0           out pkts : 0
```

```
   in bytes: 0            out bytes: 0
Assembled:
   in pkts : 0            in bytes :0
Dropped   :
   in pkts : 0            out pkts :0
   in bytes: 0            out bytes: 0
Out-of-sequence pkts: 0
```

表1-3 **display fr fragment-info interface** 命令显示信息描述表

字段	描述
Type	分片类型，包括三种：FRF.12、FRF.11 Annex C、Motorola fragment
Size	分片大小
Data-level	语音未启动时的数据报文分片大小
Voice-level	语音启动时的数据报文分片大小
Pre-fragment	需要进行分片发送的数据包数目
Fragmented	分片报文数目
Assembled	重组的分片数目
Dropped	丢弃的分片数目
Out-of-sequence pkts	乱序的分片数目
out pkts / out bytes	出方向报文数/字节数
in pkts / in bytes	入方向报文数/字节数

1.1.9 display fr switch-table

【命令】

display fr switch-table { **all** | **name** *switch-name* | **interface** *interface-type interface-number* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

all：显示所有的交换 PVC 的信息。

name *switch-name*：显示指定名称的交换 PVC 的信息。*switch-name* 表示交换 PVC 的名称，为 1～256 个字符的字符串。

interface *interface-type interface-number*：显示指定接口的交换 PVC 的信息。*interface-type interface-number* 用来指定接口类型和编号。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display fr switch-table 命令用来显示帧中继交换 PVC 状态和配置信息。

相关配置可参考命令 **fr switch**。

【举例】

显示所有配置的帧中继交换 PVC 的信息。

```
<Sysname> display fr switch-table all
Switch-Name     Interface      DLCI  Interface         DLCI  State
  test           MFR0          100    MFR1             101   UP
```

表1-4 **display fr switch-table** 命令显示信息描述表

字段	描述
Switch-Name	用于交换的PVC的名称
Interface	第一个Interface指本地接口，第二个Interface指对端接口
DLCI	第一个DLCI指本地的虚电路标识符，第二个DLCI指对端的虚电路标识符
State	帧中继交换链路的连接状态

1.1.10 display qos policy interface

【命令】

display qos policy interface [*interface-type interface-number* [**dlci** *dlci-number*] | **inbound** | **outbound**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

interface-type interface-number：指定接口类型和编号。

dlci *dlci-number*：显示指定 DLCI 应用 CBQ 的信息。*dlci-number* 表示 DLCI 编号，取值范围为 16～1007。

inbound：接口入方向应用 CBQ 的信息。

outbound：接口出方向应用 CBQ 的信息。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display qos policy interface 命令用来显示接口应用 CBQ 的信息。

【举例】

显示接口 MFR1 的 DLCI 为 25 的虚电路上应用 CBQ 的信息。

```
<Sysname> display qos policy interface mfr 1

  Interface: MFR1

  Direction: Outbound

  Policy: policy1
   Classifier: default-class
    Matched : 0(Packets) 0(Bytes)
    5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
    Rule(s) : If-match any
    Behavior:
    Default Queue:
      Flow Based Weighted Fair Queueing
        Max number of hashed queues: 256
        Matched  : 0/0 (Packets/Bytes)
        Enqueued : 0/0 (Packets/Bytes)
        Discarded: 0/0 (Packets/Bytes)
        Discard Method: Tail
   Classifier: classifier1
    Matched : 0(Packets) 0(Bytes)
    5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
    Operator: AND
    Rule(s):  If-match acl 2001
    Behavior:
      Assured Forwarding:
        Bandwidth 10 (Kbps)
        Matched  : 0/0 (Packets/Bytes)
        Enqueued : 0/0 (Packets/Bytes)
        Discarded: 0/0 (Packets/Bytes)
```

表1-5 **display qos policy interface** 命令显示信息描述表

字段	描述
Interface	应用CBQ的帧中继接口
Direction	策略应用在接口的方向
Policy	应用到接口上的策略的名称
Classifier	策略里分类规则以及对应的配置信息
Matched	符合分类规则的数据包数目
5-minute statistics	最近5分钟的流速统计信息（如果流速统计的策略超过1000个、或者流速统计的分类超过10000个，则统计信息将显示为none）
Forwarded	符合分类规则的成功转发报文在统计周期内的平均速率
Dropped	符合分类规则的丢弃报文在统计周期内的平均速率
Operator	同一个类中多条分类规则的逻辑关系
Rule(s)	类的匹配规则
Behavior	流行为的名称及对应的配置信息
Default Queue	默认队列
Flow Based Weighted Fair Queueing	基于流的加权公平队列
Max number of hashed queues	Hash队列最大数目
Matched	队列匹配的包数/字节数
Enqueued	入队包数/字节数
Discarded	丢弃包数/字节数
Discard Method	丢弃方式，共支持尾丢弃Tail、基于IP优先级的随机早期丢弃IP Precedence based WRED和基于DSCP的随机早期丢弃DSCP based WRED三种方式
Assured Forwarding	确保转发（AF队列）的相关信息
Bandwidth	AF队列可确保的最小带宽

1.1.11 display qos pvc-pq interface

【命令】

display qos pvc-pq interface [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

interface-type interface-number：指定接口类型和编号。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display qos pvc-pq interface 命令用来查看帧中继接口上的 PVC PQ 队列的信息。

【举例】

查看帧中继接口 Serial2/0 上的 PVC PQ 队列的信息。

```
<Sysname> display qos pvc-pq interface serial 2/0
Interface: Serial2/0
Output queue : (Urgent queuing : Size/Length/Discards)  0/100/0
Output queue : (Protocol queuing : Size/Length/Discards)  0/500/0
Output queue : (PVC-PQ queuing : Size/Length/Discards)
Top:  0/20/0    Middle:  0/40/0    Normal:  0/60/0    Bottom:  0/80/0
```

表1-6 **display qos pvc-pq interface** 命令显示信息描述表

字段	描述
Interface	帧中继接口
Output queue : (Urgent queuing : Size/Length/Discards)	紧急队列的出队列信息： 队列中数据包数目/队列大小/丢弃的数据包数目
Output queue : (PVC-PQ queuing: Size/Length/Discards)	PVC PQ队列的出队列信息： 队列中数据包数目/队列大小/丢弃的数据包数目
Top	高优先队列的出队列信息
Middle	中优先队列的出队列信息
Normal	正常优先队列的出队列信息
Bottom	低优先队列的出队列信息

1.1.12 ebs

【命令】

ebs [**inbound** | **outbound**] *excess-burst-size*

undo ebs [**inbound** | **outbound**]

【视图】

帧中继类视图

【缺省级别】

2：系统级

【参数】

inbound：报文入方向的超出突发尺寸，本参数仅当接口使能帧中继流量监管时有效。

outbound：报文出方向的超出突发尺寸，本参数仅当接口使能帧中继流量整形时有效。

excess-burst-size：超出突发尺寸，取值范围为 0～16000000，单位为 bit，缺省值为 0bits。

【描述】

ebs 命令用来配置帧中继虚电路的 EBS（Excess burst size，超出突发尺寸）。**undo ebs** 命令用来恢复缺省值。

EBS 为时间间隔 Tc 内报文流量超过 CBS 部分的最大值。当网络发生拥塞时，这部分超出的流量将会被优先丢弃。

在使用该命令时，如果不指定报文方向，则表示配置的 EBS 值将同时在入接口方向和出接口方向生效。

相关配置可参考命令 **cbs**、**cir allow** 和 **cir**。

【举例】

配置名为 test1 的帧中继类的超出突发尺寸为 32000bits。

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] ebs 32000
```

1.1.13 fifo queue-length

【命令】

fifo queue-length *queue-length*

undo fifo queue-length

【视图】

帧中继类视图

【缺省级别】

2：系统级

【参数】

queue-length：FIFO 队列长度，即队列能够容纳的数据报文最大个数，取值范围为 1～1024，缺省值为 40。

【描述】

fifo queue-length 命令用来配置帧中继虚电路的 FIFO（First in First out，先入先出）队列长度。**undo fifo queue-length** 命令用来恢复缺省值。

当设备作为 DCE 交换时，若 DLCI 应用了帧中继类，可以配置 DLCI 的 FIFO 队列长度。

相关配置可参考命令 **fr class**。

【举例】

配置名为 test1 的帧中继类的 FIFO 队列长度为 80。

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] fifo queue-length 80
```

1.1.14 fr class

【命令】

fr class *class-name*

undo fr class *class-name*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

class-name：帧中继类名称，为 1～30 个字符的字符串。

【描述】

fr class 命令用来创建帧中继类并进入帧中继类视图。**undo fr class** 命令用来删除指定的帧中继类。

缺省情况下，没有创建帧中继类。

只有将帧中继类同接口或虚电路相关联，并且使能相应接口的帧中继 QoS 功能，配置的帧中继类参数才会起作用。

删除帧中继类时，将释放所有接口或 DLCI 与该帧中继类的关联。

相关配置可参考命令 **fr-class**。

【举例】

创建名为 test1 的帧中继类。

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1]
```

1.1.15 fr congestion-threshold

【命令】

fr congestion-threshold { **de** | **ecn** } *queue-percentage*

undo fr congestion-threshold { **de** | **ecn** }

【视图】

帧中继接口视图/MFR 接口视图

【缺省级别】

2：系统级

【参数】

de：发生拥塞时，丢弃 DE 标志位为 1 的帧中继报文。

ecn：发生拥塞时，将帧中继报文的 BECN 和 FECN 标志位置 1。

queue-percentage：网络拥塞门限值，为接口队列的使用率。它等于接口队列当前长度占队列总长度的百分比，取值范围为 1～100，缺省值为 100。

【描述】

fr congestion-threshold 命令用来使能帧中继接口的拥塞管理功能。**undo fr congestion-threshold** 命令用来禁止该功能。

缺省情况下，禁止帧中继接口的拥塞管理功能。

本命令功能类似于命令 **congestion-threshold**，不同之处在于：本命令所应用的范围是帧中继接口，而命令 **congestion-threshold** 所应用的范围是帧中继虚电路。

相关配置可参考命令 **congestion-threshold**。

说明

本命令只能在帧中继 DCE 接口或 NNI 接口上使用。

【举例】

配置接口队列长度超过总长度 80%时，开始丢弃 DE 标志位为 1 的帧中继报文。

```
<Sysname> system-view
[Sysname]interface serial 2/0
[Sysname-Serial2/0] fr interface-type dce
[Sysname-Serial2/0] fr congestion-threshold de 80
```

1.1.16 fr de del

【命令】

fr de del *list-number* **dlci** *dlci-number*

undo fr de del *list-number* **dlci** *dlci-number*

【视图】

帧中继接口视图（主接口或子接口）/MFR 接口视图

【缺省级别】

2：系统级

【参数】

list-number：DE 规则列表编号，取值范围为 1～10。

dlci-number：帧中继虚电路编号，取值范围为 16～1007。

【描述】

fr de del 命令用来将 DE 规则列表应用到指定的帧中继虚电路上。**undo fr de del** 命令用来将 DE 规则列表从虚电路上删除。

缺省情况下，帧中继虚电路上没有应用 DE 规则列表。

需要注意的是：

- 在主接口视图下配置时只能将 DE 规则列表应用到主接口的帧中继虚电路上。在子接口视图下配置时只能将 DE 规则列表应用到子接口的帧中继虚电路上。
- 帧中继虚电路应用了 DE 规则列表后，如果有符合 DE 规则列表的报文要发送，它会将报文的 DE 标志位置 1。

相关配置可参考命令 **fr del inbound-interface** 和 **fr del protocol**。

【举例】

将 DE 规则列表 3 应用到接口 Serial2/0 的 DLCI 100 上。

```
<Sysname> system-view
[Sysname]interface serial 2/0
[Sysname-Serial2/0] fr dlci 100
[Sysname-Serial2/0] fr de del 3 dlci 100
```

1.1.17 fr del inbound-interface

【命令】

fr del *list-number* **inbound-interface** *interface-type interface-number*

undo fr del *list-number* **inbound-interface** *interface-type interface-number*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

list-number：DE 规则列表的编号，取值范围为 1～10。

interface-type interface-number：指定接口类型和编号。

【描述】

fr del inbound-interface 命令用来配置基于接口的 DE 规则列表。对于从指定接口接收的报文，如果作为帧中继报文从本设备转发，那么转发前它的 DE 标志位将被置 1。**undo fr del inbound-interface** 命令用来从 DE 规则列表内删除指定的 DE 规则。

缺省情况下，没有创建 DE 规则列表。

重复使用本命令可以为 DE 规则列表添加新的规则。每个 DE 规则列表最多可以配置 100 条规则。**undo fr del inbound-interface** 命令每次只能删除一条 DE 规则。如果要删除一个 DE 规则列表，则必须先删除列表中的所有 DE 规则。

相关配置可参考命令 **fr de del** 和 **fr del protocol**。

【举例】

在 DE 规则列表 1 内添加一条规则，对于从接口 Serial2/0 接收的报文，如果需要封装帧中继协议转发，转发前将报文的 DE 标志位置为 1。

```
<Sysname> system-view
[Sysname] fr del 1 inbound-interface serial 2/0
```

1.1.18 fr del protocol

【命令】

fr del *list-number* **protocol ip** [**acl** *acl-number* | **fragments** | **greater-than** *bytes* | **less-than** *bytes* | **tcp** *ports* | **udp** *ports*]

undo fr del *list-number* **protocol ip** [**fragments** | **acl** *acl-number* | **less-than** *bytes* | **greater-than** *bytes* | **tcp** *ports* | **udp** *ports*]

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

list-number：DE 规则列表编号，取值范围为 1～10。

protocol ip：IP 协议。

acl *acl-number*：符合 ACL 匹配条件的 IP 报文。*acl-number* 的取值范围为 2000～3999。

fragments：所有分片的 IP 报文。

greater-than *bytes*：长度大于 *bytes* 的 IP 报文。*bytes* 的取值范围为 0～65535。

less-than *bytes*：长度小于 *bytes* 的 IP 报文。*bytes* 的取值范围为 0～65535。

tcp *ports*：源或目的 TCP 端口号为 *ports* 的 IP 报文。取值范围为 0～65535。*ports* 的值既可以直接使用端口名称，也可以使用相关端口号。

udp *ports*：源或目的 UDP 端口号为 *ports* 的 IP 报文。取值范围为 0～65535。*ports* 的值既可以直接使用端口名称，也可以使用相关端口号。

【描述】

fr del protocol ip 命令用来配置基于 IP 协议的 DE 规则列表。对于封装了符合指定规则的 IP 报文的帧中继报文，将其 DE 标志位置为 1。**undo fr del protocol ip** 命令用来从 DE 规则列表内删除指定的 DE 规则。

缺省情况下，没有创建 DE 规则列表。

重复使用本命令可以为 DE 规则列表添加新的规则。每个 DE 规则列表最多可以配置 100 条规则。本命令的 **undo** 形式每次只能删除一条 DE 规则，如果要删除一个 DE 规则列表，必须把列表中的所有 DE 规则全部删除。

相关配置可参考命令 **fr de del** 和 **fr del inbound-interface**。

说明

如果不使用可选参数，则为所有 IP 报文配置 DE 规则列表。

【举例】

在 DE 规则列表 1 内添加一条规则，对所有封装 IP 报文的帧中继报文，将其 DE 标志位置为 1。

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

```
[Sysname] fr del 1 protocol ip
```

1.1.19 fr pvc-pq

【命令】

fr pvc-pq [*top-limit middle-limit normal-limit bottom-limit*]

undo fr pvc-pq

【视图】

帧中继接口视图/MFR 接口视图

【缺省级别】

2：系统级

【参数】

top-limit：高优先队列的队列长度，取值范围为 1～1024，单位为报文的个数，缺省值为 20。

middle-limit：中优先队列的队列长度，取值范围为 1～1024，单位为报文的个数，缺省值为 40。

normal-limit：正常优先队列的队列长度，取值范围为 1～1024，单位为报文的个数，缺省值为 60。

bottom-limit：低优先队列的队列长度，取值范围为 1～1024，单位为报文的个数，缺省值为 80。

【描述】

fr pvc-pq 命令用来将帧中继接口的队列类型配置为 PVC PQ（PVC Priority Queuing，虚电路优先级队列），并可以为各队列配置长度，即队列最多能容纳的报文个数。**undo fr pvc-pq** 命令用来将接口的队列类型恢复为 FIFO。

缺省情况下，帧中继接口的队列类型为 FIFO。

当接口使能帧中继流量整形功能后，接口队列类型只能为 FIFO 或者 PVC PQ。

PVC PQ 是帧中继类新增的一种队列机制，它类似于 PQ 队列，也有四种队列类型：top、middle、normal、bottom，队列优先级依次降低。在帧中继类中配置 DLCI 进入 PVC PQ 的哪个队列。当接口发生拥塞时，不同 DLCI 入不同的 PVC PQ 队列。发送时，按照队列优先级，在发送完高优先级队列中的报文之后，再发送低优先级队列中的报文。

相关配置可参考命令 **pvc-pq**。

【举例】

配置接口 Serial2/0 的队列类型为 PVC PQ。

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] fr pvc-pq
```

1.1.20 fr traffic-policing

【命令】

fr traffic-policing

undo fr traffic-policing

【视图】

帧中继接口视图/MFR 接口视图

【缺省级别】

2：系统级

【参数】

无

【描述】

fr traffic-policing 命令用来使能帧中继流量监管功能。**undo fr traffic-policing** 命令用来禁止帧中继流量监管功能。

帧中继流量监管功能只能应用在帧中继网络的 DCE 端接口的入方向。

配置流量监管时，必须先应用 **fr swithing** 命令（请参见“二层技术-广域网接入命令参考”中的“帧中继”）将 DCE 配置为帧中继交换。

相关配置可参考命令 **fr class**。

【举例】

使能接口 Serial2/0 的流量监管功能。

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] fr traffic-policing
```

1.1.21 fr traffic-shaping

【命令】

fr traffic-shaping

undo fr traffic-shaping

【视图】

帧中继接口视图/MFR 接口视图

【缺省级别】

2：系统级

【参数】

无

【描述】

fr traffic-shaping 命令用来使能帧中继流量整形功能。**undo fr traffic-shaping** 命令用来禁止帧中继流量整形功能。

缺省情况下，禁止帧中继流量整形功能。

帧中继流量整形功能应用于设备的出接口上，通常应用于帧中继网络的 DTE 端。

相关配置可参考命令 **fr class**、**fr-class** 和“二层技术-广域网接入命令参考/帧中继”中的 **fr dlci**。

【举例】

在串口 Serial2/0 上使能帧中继流量整形。

```
<Sysname> system-view
[Sysname] interface serial 2/0
```

```
[Sysname-Serial2/0] fr traffic-shaping
```

1.1.22 fr fragment end-to-end

【命令】

fr fragment [*fragment-size*] **end-to-end**

undo fr fragment

【视图】

帧中继接口视图

【缺省级别】

2：系统级

【参数】

fragment-size：FRF.12 分片报文大小，取值范围是 16～1600，单位为字节，缺省的分片报文大小为 45 字节。

【描述】

fr fragment end-to-end 命令用来使能接口 FRF.12 分片功能。**undo fr fragment** 命令用来禁止此功能。

缺省情况下，禁止接口 FRF.12 分片功能。

需要注意的是，此命令不能与 **fr traffic-shaping** 命令同时使用。

【举例】

在同步串口 Serial2/0 下使能接口 FRF.12 分片功能，不指定分片大小（采用缺省分片大小 45 字节）。

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-serial2/0] link-protocol fr
[Sysname-serial2/0] fr fragment end-to-end
```

在同步串口 Serial2/1 下使能接口 FRF.12 分片功能，指定分片大小为 300 字节。

```
<Sysname> system-view
[Sysname] interface serial 2/1
[Sysname-serial2/1] link-protocol fr
[Sysname-serial2/1] fr fragment 300 end-to-end
```

1.1.23 fragment

【命令】

fragment [*fragment-size*] [**data-level** | **voice-level**]

undo fragment [**data-level** | **voice-level**]

【视图】

帧中继类视图

【缺省级别】

2：系统级

【参数】

fragment-size：分片报文大小，取值范围为 16～1600，单位为字节，缺省的分片报文大小为 45 字节。

data-level：语音未启动条件下的分片报文大小。

voice-level：语音启动条件下的分片报文大小。

【描述】

fragment 命令用来使能帧中继虚电路的报文分片功能（符合帧中继论坛 FRF.12 标准）。**undo fragment** 命令用来禁止此功能。

缺省情况下，禁止帧中继虚电路的报文分片功能。

需要注意的是，如果没有指定参数 **data-level** 和 **voice-level**，则表示处于语音未启动条件下。

相关配置可参考命令 **fr class**。

【举例】

在名为 test1 的帧中继类下配置分片大小为 128 字节。

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] fragment 128
```

1.1.24 fr-class

【命令】

fr-class *class-name*

undo fr-class *class-name*

【视图】

帧中继 DLCI 视图/帧中继接口视图

【缺省级别】

2：系统级

【参数】

class-name：帧中继类的名称，为 1～30 个字符的字符串。

【描述】

fr-class 命令用来将帧中继类与当前帧中继虚电路或帧中继接口关联起来。**undo fr-class** 命令用来取消帧中继类与当前帧中继虚电路或帧中继接口的关联。

缺省情况下，没有帧中继类与帧中继虚电路或帧中继接口相关联。

假如指定的帧中继类不存在，此命令会先创建一个帧中继类，然后将此帧中继类和当前虚电路或接口关联起来。假如指定的帧中继类存在，此命令只会将此帧中继类和当前虚电路或接口关联，不会创建新的帧中继类。

本命令的 **undo** 形式只取消指定的帧中继类和虚电路或接口的关联，并不删除实际的帧中继类。如果要删除帧中继类，请使用 **undo fr calss** 命令。

将一个帧中继类和接口关联起来之后，此接口上的所有虚电路都会继承此帧中继类的帧中继 QoS 参数。

相关配置可参考命令 **fr class** 和“二层技术-广域网接入命令参考/帧中继”中的 **fr dlci**。

【举例】

将名为 test1 的帧中继类与 DLCI 为 200 的帧中继虚电路关联起来。

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] fr dlci 200
[Sysname-fr-dlci-Serial2/0-200] fr-class test1
```

1.1.25 pq

【命令】

pq pql *pql-index*

undo pq

【视图】

帧中继类视图

【缺省级别】

2：系统级

【参数】

pql-index：优先队列列表编号，取值范围为 1～16。

【描述】

pq 命令用来将帧中继虚电路的队列类型配置为 PQ（Priority Queuing，优先队列）。**undo pq** 命令用来将虚电路的队列类型恢复为 FIFO。

缺省情况下，帧中继虚电路的队列类型为 FIFO。

相关配置可参考命令 **cq**、**wfq** 和 **fr pvc-pq**。

【举例】

将优先队列的第 10 组应用到名为 test1 的帧中继类上。

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] pq pql 10
```

1.1.26 pvc-pq

【命令】

pvc-pq { **bottom** | **middle** | **normal** | **top** }

undo pvc-pq

【视图】

帧中继类视图

【缺省级别】

2：系统级

【参数】

bottom：低优先队列。

middle：中优先队列。

normal：正常优先队列。

top：高优先队列。

【描述】

pvc-pq 命令用来配置帧中继虚电路发送的报文进入的 PVC PQ 队列类型。**undo pvc-pq** 命令用来恢复缺省进入的 PVC PQ 队列类型。

缺省情况下，帧中继虚电路发送的报文进入的 PVC PQ 队列类型为 **normal**。

PVC PQ 队列分为 **top**、**middle**、**normal**、**bottom** 四种类型，优先级依次降低。

每个虚电路的报文只能进入一种类型的 PVC PQ 队列。

相关配置可参考命令 **fr pvc-pq**。

【举例】

配置与名为 test1 的帧中继类关联的虚电路发送的报文进入 **top** 类型的 PVC PQ 队列。

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] pvc-pq top
```

1.1.27 rtpq

【命令】

rtpq start-port *min-dest-port* **end-port** *max-dest-port* **bandwidth** *bandwidth* [**cbs** *committed-burst-size*]

undo rtpq

【视图】

帧中继类视图

【缺省级别】

2：系统级

【参数】

start-port *min-dest-port*：目的 UDP 端口的下限，取值范围为 2000～65535。

end-port *max-dest-port*：目的 UDP 端口的上限，取值范围为 2000～65535。*max-dest-port* 的值不能小于 *min-dest-port* 的值。

bandwidth *bandwidth*：RTP 队列的带宽，取值范围为 8～1000000，单位为 kbps。

cbs *committed-burst-size*：承诺突发尺寸，取值范围为 1500～2000000，单位为 byte，缺省值为 55550bytes。

【描述】

rtpq 命令用来在帧中继类上应用 RTPQ（Realtime Transport Protocol Priority Queue，优先队列）。

undo rtpq 命令用来取消在帧中继类上应用 RTPQ。

将配置了 RTPQ 的帧中继类应用到 PVC 上，将在该 PVC 上创建一个严格优先队列，目的 UDP 端口在 RTPQ 指定的端口范围内的报文将进入 RTPQ 优先队列。虚电路发生拥塞时，该队列的报文绝对优先发送，但不超过配置的带宽；虚电路没有发生拥塞时，指定端口范围内的 RTP 报文可以占用虚电路上可用带宽。一般可将 VoIP 使用的 UDP 端口范围配置为[16384，32767]。

【举例】

在名为 test1 的帧中继类上配置 RTPQ，带宽为 20kbps。

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] rtpq start-port 16383 end-port 16384 bandwidth 20
```

1.1.28 traffic-shaping adaptation

【命令】

traffic-shaping adaptation { **becn** *percentage* | **interface-congestion** *number* }

undo traffic-shaping adaptation { **becn** | **interface-congestion** }

【视图】

帧中继类视图

【缺省级别】

2：系统级

【参数】

becn：对带 BECN 标志的报文进行流量调节。

percentage：每次调节的比例（百分比），取值范围为 1～30，缺省值为 25。

interface-congestion：根据接口出队列中的报文数进行流量调节。

number：接口出队列中的报文个数，取值范围为 1～40。

【描述】

traffic-shaping adaptation 命令用来使能帧中继流量整形的自适应流量调节功能。**undo traffic-shaping adaptation** 命令用来禁止此功能。

缺省情况下，使能对带 BECN 标志的报文进行自适应流量调节功能，每次调节的比例为 25。

相关配置可参考命令 **fr traffic-shaping**、**cir allow** 和 **cir**。

【举例】

使能帧中继流量整形的自适应流量调节功能，对 BECN 位为 1 的报文进行调节，每次调节的比例为 20。

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] traffic-shaping adaptation becn 20
```

1.1.29 wfq

【命令】

wfq [*congestive-discard-threshold* [*dynamic-queues*]]

undo wfq

【视图】

帧中继类视图

【缺省级别】

2：系统级

【参数】

congestive-discard-threshold：WFQ 队列中数据报文的最大个数，超出此个数，数据报文将被丢弃。取值范围为 1～1024，缺省值为 64。

dynamic-queues：WFQ 队列的总数。可取值为 16、32、64、128、256、512、1024、2048 与 4096，缺省值为 256。

【描述】

wfq 命令用来将帧中继虚电路的队列类型配置为 WFQ（Weighted Fair Queuing，加权公平队列）。**undo wfq** 命令用来将虚电路的队列类型恢复为 FIFO。

缺省情况下，虚电路的队列类型为 FIFO。

相关配置可参考命令 **cq**、**pq** 和 **fr pvc-pq**。

【举例】

将加权公平队列应用到名为 test1 的帧中继类上，队列中数据报文的最大个数为 128，队列总数为 512。

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] wfq 128 512
```

目 录

1 MPLS QoS

1.1 MPLS QoS配置命令

1.1.1 if-match mpls-exp

【命令】

if-match [**not**] **mpls-exp** *exp-value-list*

undo if-match [**not**] **mpls-exp** *exp-value-list*

【视图】

类视图

【缺省级别】

2：系统级

【参数】

not：不匹配该规则。

exp-value-list：EXP 值的列表，取值范围为 0～7，最多可以配置 8 个 EXP 值。如果指定了多个相同的 EXP 值，系统默认为一个；多个不同的 EXP 值是或的关系，即只要有一个值匹配，就算匹配这条规则。

【描述】

if-match mpls-exp 命令用来定义匹配 MPLS EXP 优先级的规则。**undo if-match mpls-exp** 命令用来删除匹配 MPLS EXP 优先级的规则。

【举例】

定义匹配 EXP 优先级为 3 或 4 的报文的规则。

```
<Sysname> system-view
[Sysname] traffic classifier database
[Sysname-classifier-database] if-match mpls-exp 3 4
```

1.1.2 qos cql protocol mpls exp

【命令】

qos cql *cql-index* **protocol mpls exp** *exp-value-list* **queue** *queue-number*

undo qos cql *cql-index* **protocol mpls exp** *exp-value-list*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

cql-index：定制列表的组号，取值范围为 1～16。

queue *queue-number*：定制队列的队列号，取值范围为 0～16。

exp-value-list：EXP 值的列表，取值范围为 0～7，用户可以重复输入 8 个 EXP 值。

【描述】

qos cql protocol mpls exp 命令用来配置基于 MPLS 协议的定制队列分类规则。**undo qos cql protocol mpls exp** 命令用来删除相应的定制分类规则。

需要注意的是：

- 对于同一个 *cql-index*，本命令可以重复使用，从而为同一个优先列表配置多种分类规则。
- 当存在多个规则时，设备以规则的配置顺序来匹配数据包。

【举例】

配置基于 MPLS 协议的定制列表 10 的分类规则，设置队列 2 对应 EXP 值 1。

```
<Sysname> system-view
[Sysname] qos cql 10 protocol mpls exp 1 queue 2
```

1.1.3 qos pql protocol mpls exp

【命令】

qos pql *pql-index* **protocol mpls exp** *exp-value-list* **queue** { **bottom** | **middle** | **normal** | **top** }

undo qos pql *pql-index* **protocol mpls exp** *exp-value-list*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

pql-index：优先列表的组号，取值范围为 1～16。

top、**middle**、**normal**、**bottom**：对应 PQ 的四个队列，优先级依次降低。

exp-value-list：EXP 值的列表，取值范围为 0～7，用户可以重复输入 8 个 EXP 值。

【描述】

qos pql protocol mpls exp 命令用来配置基于 MPLS 协议的优先列表分类规则。**undo qos pql protocol mpls exp** 命令用来删除相应的优先列表分类规则。

需要注意的是：

- 对于同一个 *pql-index*，本命令可以重复使用，从而为同一个优先列表配置多种分类规则。
- 当存在多个规则时，设备以规则的配置顺序来匹配数据包。

相关配置可参考命令 **qos pql protocol**。

【举例】

配置基于 MPLS 协议的优先列表 10 分类规则，设置队列 top 对应的 EXP 值为 5。

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

```
[Sysname] qos pql 10 protocol mpls exp 5 queue top
```

1.1.4 remark mpls-exp

【命令】

remark mpls-exp *exp-value*

undo remark mpls-exp

【视图】

流行为视图

【缺省级别】

2：系统级

【参数】

exp-value：MPLS 报文的 EXP 值，取值范围为 0～7。

【描述】

remark mpls-exp 命令用来配置标记 MPLS 报文的 EXP 值。**undo remark mpls-exp** 命令用来取消标记 MPLS 报文的 EXP 值。

【举例】

配置标记 MPLS 报文的 EXP 值为 0。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark mpls-exp 0
```