H3C S5830 系列以太网交换机

ACL 和 QoS 命令参考

杭州华三通信技术有限公司
http://www.h3c.com.cn

资料版本：6W102-20141223
产品版本：Release 1115&Release 1118

H3C、  、H3CS、H3CIE、H3CNE、Aolynk、  、H^{3}Care、  、IRF、NetPilot、Netflow、SecEngine、SecPath、SecCenter、SecBlade、Comware、ITCMM、HUASAN、华三均为杭州华三通信技术有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。H3C 保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，H3C 尽全力在本手册中提供准确的信息，但是 H3C 并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前 言

H3C S5830 系列以太网交换机命令参考共分为十本手册，主要针对 S5830 Release 1115&Release 1118 软件版本支持的命令进行了介绍。《ACL 和 QoS 命令参考》主要介绍了配置 ACL 和 QoS 功能时涉及的各种命令，包括创建 ACL、配置 QoS 策略，以及配置流量监管、流量整形、拥塞管理、拥塞避免等常用 QoS 技术时所使用的命令。

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. 端口编号示例约定

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

资料获取方式

您可以通过H3C网站（www.h3c.com.cn）获取最新的产品资料：

H3C 网站与产品资料相关的主要栏目介绍如下：

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

技术支持

用户支持邮箱：service@h3c.com

技术支持热线电话：400-810-0504（手机、固话均可拨打）

网址：http://www.h3c.com.cn

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 ACL

说明

本文中的三层以太网端口是指工作模式被配置成三层模式的以太网端口，有关以太网端口工作模式切换的操作，请参见“二层技术-以太网交换配置指导”中的“以太网端口配置”部分。

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：

- 2000～2999：表示 IPv4 基本 ACL；
- 3000～3999：表示 IPv4 高级 ACL；
- 4000～4999：表示二层 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。

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。

all：指定全部 ACL（包括 IPv4 基本 ACL、IPv4 高级 ACL 和二层 ACL）。

【描述】

acl 命令用来创建一个 IPv4 基本 ACL、IPv4 高级 ACL 或二层 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 IPv4 基本 ACL、IPv4 高级 ACL 和二层 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：

- 2000～2999：表示 IPv4 基本 ACL；
- 3000～3999：表示 IPv4 高级 ACL；
- 4000～4999：表示二层 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。

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：

- 2000～2999：表示 IPv4 基本 ACL；
- 3000～3999：表示 IPv4 高级 ACL；
- 4000～4999：表示二层 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。

【描述】

acl copy 命令用来复制并生成新的 IPv4 基本 ACL、IPv4 高级 ACL 或二层 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 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。

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。

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。

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

【描述】

acl ipv6 命令用来创建一个 IPv6 基本 ACL 或 IPv6 高级 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 和 IPv6 高级 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 或二层 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 或二层 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】

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

【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**。

【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* } [**slot** *slot-number*] [**|** { **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：

- 2000～2999：表示 IPv4 基本 ACL；
- 3000～3999：表示 IPv4 高级 ACL；
- 4000～4999：表示二层 ACL。

all：显示全部 ACL（包括 IPv4 基本 ACL、IPv4 高级 ACL 和二层 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。

slot *slot-number*：显示指定成员设备上 ACL 的运行情况，*slot-number* 表示设备在 IRF 中的成员编号。若未指定本参数，将显示 IRF 设备整体的 ACL 配置情况。

|：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 IPv4 基本 ACL、IPv4 高级 ACL 和二层 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 IPv4 基本 ACL、IPv4 高级 ACL 和二层 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： • Basic ACL：表示 IPv4 基本 ACL • Advanced ACL：表示 IPv4 高级 ACL • Ethernet frame ACL：表示二层 ACL
named flow	该ACL的名称为flow，-none-表示没有名称
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
Statistics is enabled	该ACL基于硬件应用时的规则匹配统计功能已使能
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，在ACL规则中未配置**counting**参数且在ACL视图下未配置**hardware-count enable**命令的情况下，此处仅统计软件IPv4 ACL的匹配次数；如果配置了**counting**参数或**hardware-count enable**命令，则此处将统计基于软件和基于硬件应用的IPv4 ACL的匹配次数之和（匹配次数为0时不显示本字段）
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* } [**slot** *slot-number*] [**|** { **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。

all：显示全部 ACL（包括 IPv6 基本 ACL 和 IPv6 高级 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。

slot *slot-number*：显示指定成员设备上 ACL 的运行情况，*slot-number* 表示设备在 IRF 中的成员编号。若未指定本参数，将显示 IRF 设备整体的 ACL 配置情况。

|：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 和 IPv6 高级 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 和 IPv6 高级 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 rd
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
named flow	该ACL的名称为flow，-none-表示没有名称
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
Statistics is enabled	该ACL基于硬件应用时的规则匹配统计功能已使能
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，在ACL规则中未配置**counting**参数且在ACL视图下未配置**hardware-count enable**命令的情况下，此处仅统计软件IPv6 ACL的匹配次数；如果配置了**counting**参数或**hardware-count enable**命令，则此处将统计基于软件和基于硬件应用的IPv6 ACL的匹配次数之和（匹配次数为0时不显示本字段）
rule 10 comment This rule is used in VPN rd.	规则10的描述信息

1.1.10 display acl resource

【命令】

display acl resource [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

slot *slot-number*：显示指定成员设备上 ACL 资源的使用情况，*slot-number* 表示设备在 IRF 中的成员编号。若未指定本参数，将显示 IRF 中所有成员设备上 ACL 资源的使用情况。

|：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 resource 命令用来显示 ACL 资源的使用情况。

【举例】

显示设备上 ACL 资源的使用情况。

```
<Sysname> display acl resource
Interface:
   GE1/0/1 to GE1/0/24
-------------------------------------------------------------------------
 Type          Total       Reserved    Configured  Remaining   Usage
-------------------------------------------------------------------------
 VFP ACL       2048        512         0           1536        25%
 IFP ACL       4096        1024        1           3071        25%
 IFP Meter     2048        512         0           1536        25%
 IFP Counter   2048        512         0           1536        25%
 EFP ACL       512         0           1           511         0%
 EFP Meter     256         0           0           256         0%
 EFP Counter   512         0           0           512         0%

 Interface:
   GE1/0/25 to GE1/0/50, XGE1/0/51 to XGE1/0/52
-------------------------------------------------------------------------
 Type          Total       Reserved    Configured  Remaining   Usage
-------------------------------------------------------------------------
 VFP ACL       2048        512         0           1536        25%
 IFP ACL       4096        1024        0           3072        25%
 IFP Meter     2048        512         0           1536        25%
 IFP Counter   2048        512         0           1536        25%
 EFP ACL       512         0           0           512         0%
 EFP Meter     256         0           0           256         0%
 EFP Counter   512         0           0           512         0%
```

表1-3 display acl resource 命令显示信息描述表

字段	描述
Interface	使用ACL资源的端口

字段	描述
Type	资源类型： • ACL 表示 ACL 规则资源 • Meter 表示流量监管资源 • Counter 表示流量统计资源 • VFP 表示二层转发前的，应用于 QinQ 功能的资源数目 • IFP 表示入方向的资源数目 • EFP 表示出方向的资源数目
Total	支持的ACL规则总数
Reserved	预留的ACL规则数
Configured	已经配置的ACL规则数
Remaining	剩余可用的ACL规则数
Usage	ACL规则的使用率

1.1.11 display packet-filter

【命令】

display packet-filter { { **all** | **interface** *interface-type interface-number* } [**inbound** | **outbound**] | **interface vlan-interface** *vlan-interface-number* [**inbound** | **outbound**] [**slot** *slot-number*] } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

all：显示所有接口上 ACL 在报文过滤中的应用情况。

interface *interface-type interface-number*：显示指定接口上 ACL 在报文过滤中的应用情况。*interface-type interface-number* 表示接口类型和接口编号，这里的接口类型不包括 VLAN 接口。

inbound：显示接口入方向上 ACL 在报文过滤中的应用情况。

outbound：显示接口出方向上 ACL 在报文过滤中的应用情况。

interface vlan-interface *vlan-interface-number*：显示指定 VLAN 接口上 ACL 在报文过滤中的应用情况。*vlan-interface-number* 表示 VLAN 接口的编号。

slot *slot-number*：显示指定成员设备的 VLAN 接口上 ACL 在报文过滤中的应用情况，*slot-number* 表示设备在 IRF 中的成员编号。若未指定本参数，将显示 IRF 设备的 VLAN 接口上 ACL 在报文过滤中的应用情况。

|：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 packet-filter 命令用来显示 ACL 在报文过滤中的应用情况。

需要注意的是：

- 在 IRF 环境下，由于各成员设备可用的 ACL 资源不同，可能出现应用到 VLAN 接口的报文过滤策略在 Master 设备和其它成员设备上应用成功或失败的结果不同的情况，此时需要使用 **slot** 参数来定位应用失败的成员设备。
- 若未指定 **inbound** 和 **outbound** 参数，将同时显示接口出、入方向上报文过滤策略的应用情况。

【举例】

显示接口 GigabitEthernet1/0/1 出、入方向上 ACL 在报文过滤中的应用情况。

```
<Sysname> display packet-filter interface gigabitethernet 1/0/1
  Interface: GigabitEthernet1/0/1
  In-bound Policy:
    acl 2001, Successful
  Out-bound Policy:
    acl6 2500, Fail
```

表1-4 display packet-filter 命令显示信息描述表

字段	描述
Interface	应用ACL进行报文过滤的接口名称
In-bound Policy	入方向上ACL在报文过滤中的应用情况
Out-bound Policy	出方向上ACL在报文过滤中的应用情况
acl 2001, Successful	IPv4基本ACL 2001应用成功
acl6 2500, Fail	IPv6基本ACL 2500应用失败

1.1.12 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1-5 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
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

1.1.13 hardware-count enable

【命令】

hardware-count enable

undo hardware-count enable

【视图】

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

【缺省级别】

2：系统级

【参数】

无

【描述】

hardware-count enable 命令用来使能基于硬件应用的 ACL 规则匹配统计功能。**undo hardware-count enable** 命令用来关闭基于硬件应用的 ACL 规则匹配统计功能。

缺省情况下，基于硬件应用的 ACL 规则匹配统计功能处于关闭状态。

需要注意的是：

- **hardware-count enable** 命令用于统计基于硬件应用的 ACL 匹配次数，基于软件应用的 ACL 匹配次数设备将自动进行统计，无需配置。
- 当 ACL 被 QoS 策略引用对报文进行流分类时，规则匹配统计功能将不能生效。
- 本命令用于控制当前 ACL 内所有规则的匹配统计功能，而 **rule** 命令中的 **counting** 参数则用于控制当前规则的匹配统计功能。对于某条规则而言，这两个配置中只要有一个处于使能状态，该规则的统计功能就会生效。
- 使用 **undo hardware-count enable** 命令会同时将该 ACL 内所有规则的统计计数清零，不论这些规则是否配置有 **counting** 参数。

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

【举例】

使能 IPv4 基本 ACL 2000 的规则匹配统计功能。

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

使能 IPv6 基本 ACL 2000 的规则匹配统计功能。

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

1.1.14 packet-filter

【命令】

packet-filter { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }

undo packet-filter { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }

【视图】

二层以太网端口视图/三层以太网端口视图/VLAN 接口视图

【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：

- 2000～2999：表示 IPv4 基本 ACL；
- 3000～3999：表示 IPv4 高级 ACL；
- 4000～4999：表示二层 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。

inbound：对接口收到的报文进行过滤。

outbound：对接口发出的报文进行过滤。

【描述】

packet-filter 命令用来在接口上应用指定的 IPv4 基本 ACL、IPv4 高级 ACL 或二层 ACL 进行报文过滤。**undo packet-filter** 命令用来取消在接口上应用指定的 IPv4 基本 ACL、IPv4 高级 ACL 或二层 ACL 进行报文过滤。

缺省情况下，接口不对报文进行过滤。

需要注意的是，请避免多个用户同时进行本配置，否则可能导致配置失败。

相关配置可参考命令 **display packet-filter**。

说明

- Release 1118P05 版本之前，在 VLAN 接口上应用 ACL 进行报文过滤时，对通过该接口进行三层转发的报文进行过滤，而对纯二层转发的报文不进行过滤。
- Release 1118P05 及以上版本，在 VLAN 接口上应用 ACL 进行报文过滤时，对通过该接口进行二、三层转发的报文均生效。

【举例】

应用 IPv4 基本 ACL 2001 对接口 GigabitEthernet1/0/1 收到的报文进行过滤。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] packet-filter 2001 inbound
```

1.1.15 packet-filter ipv6

【命令】

packet-filter ipv6 { *acl6-number* | **name** *acl6-name* } { **inbound** | **outbound** }

undo packet-filter ipv6 { *acl6-number* | **name** *acl6-name* } { **inbound** | **outbound** }

【视图】

二层以太网端口视图/三层以太网端口视图/VLAN 接口视图

【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。

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。

inbound：对接口收到的 IPv6 报文进行过滤。

outbound：对接口发出的 IPv6 报文进行过滤。

【描述】

packet-filter ipv6 命令用来在接口上应用指定的 IPv6 基本 ACL 或 IPv6 高级 ACL 进行报文过滤。**undo packet-filter ipv6** 命令用来取消在接口上应用指定的 IPv6 基本 ACL 或 IPv6 高级 ACL 进行报文过滤。

缺省情况下，接口不对报文进行过滤。

需要注意的是，请避免多个用户同时进行本配置，否则可能导致配置失败。

相关配置可参考命令 **display packet-filter**。

说明

- Release 1118P05 版本之前，在 VLAN 接口上应用 ACL 进行报文过滤时，对通过该接口进行三层转发的报文进行过滤，而对纯二层转发的报文不进行过滤。
- Release 1118P05 及以上版本，在 VLAN 接口上应用 ACL 进行报文过滤时，对通过该接口进行二、三层转发的报文均生效。

【举例】

应用 IPv6 基本 ACL 2500 对接口 GigabitEthernet1/0/1 收到的报文进行过滤。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] packet-filter ipv6 2500 inbound
```

1.1.16 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：

- 2000～2999：表示 IPv4 基本 ACL。
- 3000～3999：表示 IPv4 高级 ACL。
- 4000～4999：表示二层 ACL。

all：指定全部 ACL（包括 IPv4 基本 ACL、IPv4 高级 ACL 和二层 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 IPv4 基本 ACL、IPv4 高级 ACL 和二层 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
```

1.1.17 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 命令用来清除指定或全部 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
```

1.1.18 rule (Ethernet frame header ACL view)

【命令】

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

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，该参数用于统计基于硬件应用的 ACL 的规则匹配次数。

dest-mac *dest-address dest-mask*：指定目的 MAC 地址范围。*dest-address* 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。

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

time-range *time-range-name*：指定本规则生效的时间段。*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**。

说明

当二层 ACL 用于 QoS 策略的流分类或用于报文过滤功能时，如果使用 **lsap** 参数，则 *lsap-type* 必须为 AAAA，*lsap-type-mask* 必须为 FFFF，否则 ACL 将无法正常应用。

【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
```

1.1.19 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 1-6 所示的规则信息参数。

表1-6 规则信息参数

参数	类别	作用	说明
source { *source-address source-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-address dest-wildcard* | **any** }	目的地址	指定ACL规则的目的地址信息	*dest-addr*：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	该参数用于统计基于硬件应用的ACL中某条规则的匹配次数
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）、**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

参数	类别	作用	说明
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	指定本规则生效的时间段	*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 1-7 所示的规则信息参数。

表1-7 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** *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） 如果在一条规则中设置了多个TCP标志位的匹配值，则这些匹配条件之间的关系为“与”

参数	类别	作用	说明
established	TCP连接建立标识	定义对TCP连接报文的处理规则	该参数用于定义TCP报文中ACK或RST标志位为1的报文

当*protocol*为**icmp**（1）时，用户还可配置如 表 1-8 所示的规则信息参数。

表1-8 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 1-9所示

表1-9 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
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**。

说明

当 IPv4 高级 ACL 用于 QoS 策略的流分类或用于报文过滤功能时：

- 不支持配置 **vpn-instance** 参数
- 不支持配置操作符 *operator* 取值为 **neq**
- 当 ACL 用于流分类时，在规则中配置的 **logging** 和 **counting** 参数不会生效

【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。

```
<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
```

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
```

1.1.20 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：表示对规则匹配情况进行统计，该参数用于统计基于硬件应用的 ACL 的规则匹配次数。

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 { *source-address source-wildcard* | **any** }：指定规则的源地址信息。*source-address* 表示报文的源 IP 地址，*source-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*：指定本规则生效的时间段。*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**。

说明

- 当 IPv4 基本 ACL 被 QoS 策略引用对报文进行流分类时，不支持配置 **vpn-instance** 参数，在规则中配置的 **logging** 和 **counting** 参数不会生效。
- 当 IPv4 基本 ACL 被用于报文过滤时，不支持配置 **vpn-instance** 参数。

【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
```

1.1.21 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 1-10 所示的规则信息参数。

表1-10 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-address*：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
counting	统计	使能本规则的匹配统计功能，缺省为关闭	该参数用于统计基于硬件应用的ACL中某条规则的匹配次数
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

参数	类别	作用	说明
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 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	指定本规则生效的时间段	*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 1-11 所示的规则信息参数。

表1-11 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**

参数	类别	作用	说明
destination-port *operator port1* [*port2*]	目的端口	定义TCP/UDP报文的目的端口信息	（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）
{ **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） 如果在一条规则中设置了多个TCP标志位的匹配值，则这些匹配条件之间的关系为“与”
established	TCP连接建立标识	定义对TCP连接报文的处理规则	该参数用于定义TCP报文中ACK或RST标志位为1的报文

当*protocol*为**icmpv6**（58）时，用户还可配置如 表 1-12 所示的规则信息参数。

表1-12 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1-13所示

表1-13 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

ICMPv6 消息名称	ICMPv6 消息类型	ICMPv6 消息码
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**。

说明

当 IPv6 高级 ACL 用于 QoS 策略的流分类或用于报文过滤功能时：

- 不支持配置 **fragment** 和 **vpn-instance** 参数
- 不支持配置操作符 *operator* 取值为 **neq**
- 如果 QoS 策略或报文过滤功能应用于出方向，则不支持配置 **flow-label** 参数
- 当 ACL 用于流分类时，在规则中配置的 **logging** 和 **counting** 参数不会生效

【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。

```
<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
```

1.1.22 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，该参数用于统计基于硬件应用的 ACL 的规则匹配次数。

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*：指定本规则生效的时间段。*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**。


说明

- 当 IPv6 基本 ACL 被 QoS 策略引用对报文进行流分类时，不支持配置 **fragment**、**routing** 和 **vpn-instance** 参数，在规则中配置的 **logging** 和 **counting** 参数不会生效。
- 当 IPv6 基本 ACL 被用于报文过滤时，不支持配置 **fragment**、**routing** 和 **vpn-instance** 参数。

【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
```

1.1.23 rule comment

【命令】

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

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

【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

【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 GigabitEthernet 1/0/1.
```

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 GigabitEthernet 1/0/1.
```

1.1.24 rule remark

【命令】

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

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

【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

【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。

1.1.25 step

【命令】

step *step-value*

undo step

【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

【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
```

1.1.26 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

说明

QoS 策略功能中的“端口”包括二层以太网端口和三层以太网端口。三层以太网端口是指被配置为三层模式的以太网端口，有关以太网端口模式切换的操作，请参见“二层技术-以太网交换配置指导”中的“以太网端口配置”。

1.1 定义类的命令

1.1.1 display traffic classifier

【命令】

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

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

user-defined：用户定义类。

tcl-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
```

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 *match-criteria*

undo if-match *match-criteria*

【视图】

类视图

【缺省级别】

2：系统级

【参数】

match-criteria：类的匹配规则，具体情况如 表 1-2 所示。

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2000～3999，IPv6 ACL序号的取值范围是2000～3999，二层ACL序号的取值范围是4000～4999 *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
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或表1-4中的关键字
destination-mac *mac-address*	定义匹配目的MAC地址的规则
customer-dot1p *8021p-list*	定义匹配内层VLAN Tag的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

取值	描述
service-dot1p *8021p-list*	定义匹配外层VLAN Tag的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
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
protocol *protocol-name*	定义匹配协议的规则，*protocol-name*取值为ip或ipv6
source-mac *mac-address*	定义匹配源MAC地址的规则
customer-vlan-id { *vlan-id-list* | *vlan-id1* **to** *vlan-id2* }	定义匹配内层VLAN Tag的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*的值必须小于*vlan-id2*的值，VLAN ID取值范围为1～4094
service-vlan-id { *vlan-id-list* | *vlan-id1* **to** *vlan-id2* }	定义匹配外层VLAN Tag的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*的值必须小于*vlan-id2*的值，VLAN ID取值范围为1～4094

说明

使用 **if-match** 命令定义匹配规则时，请注意：

- 除匹配 **customer-vlan-id**、**service-vlan-id**、**acl** 外，对于其他匹配条件，只有当流分类中各规则之间的逻辑关系指定为 **or** 时，用户才可以通过重复执行 **if-match** 命令来配置多条匹配不同取值的规则，或在一条 **if-match** 命令中使用 *list* 形式输入多个匹配值。
- 当流分类中各规则之间的逻辑关系为 **and** 时，可在一个流分类下配置多条 **if-match customer-vlan-id** 的匹配规则或在一条 **if-match** 命令中用 *list* 形式输入多个匹配值，但这些匹配规则之间或匹配值之间的逻辑关系实际为 **or**。配置多条 **if-match service-vlan-id** 规则时的情况与之相同。
- 当流分类中各规则之间的的逻辑关系为 **and** 时，可在一个流分类下配置多条 **if-match acl** 的匹配规则，但这些匹配规则之间的逻辑关系实际为 or。若在一个流分类下，匹配的一条 ACL 中包含多条规则，则多条匹配规则之间的逻辑关系为 **or**。

【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。

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。
- 当一个类下配置多条这样的命令时，各个配置之间互相不覆盖。
- 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 地址和源 MAC 地址规则

- 当一个类下配置多条这样的命令时，各个配置之间互相不覆盖。

(3) 定义匹配 DSCP 的规则

- 当一个类下配置多条这样的命令时，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。
- 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。

(4) 定义匹配内层 VLAN Tag 的或内层 VLAN Tag 的的 802.1p 优先级的规则

- 当一个类下配置多条这样的命令时，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。
- 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。

(5) 定义匹配 IP 优先级的规则

- 当一个类下配置多条这样的命令时，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。
- 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。

(6) 定义匹配内层 VLAN Tag 的或内层 VLAN Tag 的 VLAN ID 的规则

- 当一个类下配置多条这样的命令时，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 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：匹配内层 VLAN Tag 的 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 class1 的匹配规则为：匹配外层 VLAN Tag 的 802.1p 优先级为 5。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match service-dot1p 5
```

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 operator or
[Sysname-classifier-class1] if-match dscp 1
[Sysname-classifier-class1] if-match dscp 6
[Sysname-classifier-class1] if-match dscp 9
```

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 operator or
[Sysname-classifier-class1] if-match ip-precedence 1
[Sysname-classifier-class1] if-match ip-precedence 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：匹配内层 VLAN Tag 的 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 class1 的匹配规则为：匹配外层 VLAN Tag 的 VLAN ID 值为 2 或 7 或 10 的报文。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match service-vlan-id 2 7 10
```

1.1.3 traffic classifier

【命令】

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

undo traffic classifier *tcl-name*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

tcl-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**。

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]
```

1.2 定义流行为的命令

1.2.1 accounting

【命令】

accounting { **byte** | **packet** }

undo accounting

【视图】

流行为视图

【缺省级别】

2：系统级

【参数】

byte：表示报文基于字节为单位进行统计。

packet：表示报文基于包为单位进行统计。

【描述】

accounting 命令用来为流行为配置流量统计动作。**undo accounting** 命令用来取消流量统计动作配置。

相关统计信息可以通过命令 **display qos policy interface** 和 **display qos vlan-policy** 查看。

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

【举例】

为流行为配置流量统计动作，并指定统计单位为 byte。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] accounting byte
```

1.2.2 car

【命令】

car cir *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**pir** *peak-information-rate*] [**green** *action*] [**yellow** *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，取值范围为 64～10000000 且必须是 64 的倍数。

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

- 如果不指定 **cbs** 参数，缺省取值为 62.5 × *committed-information-rate*，但是最大值不能超过 16000000。
- 如果指定 **cbs** 参数，取值范围 4000～16000000。

ebs *excess-burst-size*：超出突发尺寸，取值范围为 0～16000000，缺省值为 4000byte。

pir *peak information rate*：峰值速率，单位为 kbps，取值范围为 64～10000000 且必须是 64 的倍数。

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**。

yellow *action*：数据包的流量不符合承诺速率但是符合峰值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 或 表 1-4 中的关键字。

【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。

在端口上应用的策略中使用 **car** 时，可以应用到端口报文的接收或者发送方向。

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 128kbps，承诺突发尺寸为 50000bytes，速率大于 128kbps 时，报文 DSCP 优先级改为 0 并发送。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] car cir 128 cbs 50000 ebs 0 green pass red remark-dscp-pass 0
```

1.2.3 display traffic behavior

【命令】

display traffic behavior 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】

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: 2
      Accounting enable: byte
      Committed Access Rate:
        CIR 12800 (kbps), CBS 4000 (byte), EBS 4000 (byte)
        Green Action: pass
        Red Action: discard
```

```
  Yellow Action: pass
Redirect enable:
  Redirect type: cpu
  Redirect destination: cpu
Marking:
  Remark dot1p COS 1
Marking:
  Remark DSCP af12
```

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
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、dot1p COS、local precedence、drop precedence、Customer VLAN ID、Service VLAN ID等类型，相关类型描述请参考1.2 定义流行为的命令
Accounting enable	流量统计相关信息。统计单位可以配置字节（byte）和报文个数（packet）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1.2.2 car
Red Action	对红色报文的处理，具体请参考1.2.2 car
Yellow Action	对黄色报文的处理，具体请参考1.2.2 car
Redirect enable	流量重定向相关信息
Redirect type	重定向类型，目前支持CPU、interface、next-hop三种
Redirect destination	重定向的目的。对应不同的重定向类型，可以显示为cpu、端口名称、或者下一跳的IP地址

1.2.4 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
```

1.2.5 redirect

【命令】

redirect { **cpu** | **interface** *interface-type interface-number* | **next-hop** { *ipv4-add1* [*ipv4-add2*] | *ipv6-add1* [*interface-type interface-number*] [*ipv6-add2* [*interface-type interface-number*]] } }

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

【视图】

流行为视图

【缺省级别】

2：系统级

【参数】

cpu：重定向到 CPU。

interface：重定向到指定的端口。

interface-type interface-number：指定端口类型和端口编号。

next-hop：重定向到指定的下一跳。

ipv4-add：下一跳 IPv4 地址。*ipv4-add2* 是 *ipv4-add1* 的备份下一跳地址，如果重定向到 *ipv4-add1* 失败，则会选择重定向到 *ipv4-add2*。

ipv6-add：下一跳 IPv6 地址。IPv6 地址为链路本地地址时，下一跳 IPv6 地址需要配置接口；IPv6 地址为非链路本地地址时，下一跳 IPv6 地址不需要配置接口。*ipv6-add2* 是 *ipv6-add1* 的备份下一跳地址，如果重定向到 *ipv6-add1* 失败，则会选择重定向到 *ipv6-add2*。

【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。

注意

- 在配置重定向动作时，同一个流行为中重定向类型只能为重定向到 CPU、重定向到端口和重定向到下一跳中的一种。
- 如果不配置重定向下一跳失败的处理动作，默认的处理动作是转发。

【举例】

为流行为配置流量重定向动作，重定向到 GigabitEthernet1/0/1。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] redirect interface gigabitethernet1/0/1
```

1.2.6 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
```

1.2.7 remark drop-precedence

【命令】

remark drop-precedence *drop-precedence-value*

undo remark drop-precedence

【视图】

流行为视图

【缺省级别】

2：系统级

【参数】

drop-precedence-value：标记的丢弃优先级，取值范围为 0～2。

【描述】

remark drop-precedence 命令用来配置标记报文的丢弃优先级。**undo remark drop-precedence** 命令用来取消标记报文的丢弃优先级。

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

【举例】

配置标记报文的丢弃优先级值为 2。

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

1.2.8 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

关键字	DSCP 值（二进制）	DSCP 值（十进制）
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
```

1.2.9 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
```

1.2.10 remark local-precedence

【命令】

remark local-precedence *local-precedence*

undo remark local-precedence

【视图】

流行为视图

【缺省级别】

2：系统级

【参数】

local-precedence：标记的本地优先级，取值范围为 0～7。

【描述】

remark local-precedence 命令用来配置标记报文的本地优先级。**undo remark local-precedence** 命令用来取消标记报文的本地优先级。

需要注意的是，**remark local-precedence** 动作与 **remark dot1p** 动作同时配置时，两者重标记的本地优先级和 802.1p 优先级的取值必须相同，否则策略将不能成功应用。

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

【举例】

配置标记报文的本地优先级值为 2。

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

1.2.11 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。

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]
```

1.3 定义策略和应用策略的命令

1.3.1 classifier behavior

【命令】

classifier *tcl-name* **behavior** *behavior-name* [**mode dot1q-tag-manipulation**]

undo classifier *tcl-name*

【视图】

策略视图

【缺省级别】

2：系统级

【参数】

tcl-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。

mode dot1q-tag-manipulation：设置该类和流行为对应关系用于 VLAN 映射功能。有关 VLAN 映射功能的介绍，请参见“二层技术-以太网交换配置指导”中的“VLAN 映射”。

【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。

说明

当用户在策略下配置了多组类和流行为的对应关系时，如果某个流行为中配置了 **nest**、**remark customer-vlan-id** 或 **remark service-vlan-id** 动作，建议用户不要在此流行为中配置其他动作，以保证应用策略后实际的运行结果与用户的配置意图一致。

相关配置可参考命令 **qos 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]
```

1.3.2 display qos policy

【命令】

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

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

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，则显示所有用户定义策略的配置信息。

tcl-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: 1
   Behavior: be
    -none-

 Classifier: USER1
   Behavior: USER1
    Committed Access Rate:
      CIR 256 (kbps), CBS 15000 (byte), EBS 0 (byte)
      Green Action: pass
      Red  Action: discard
    Marking:
```

```
Remark IP Precedence 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

1.3.3 display qos policy global

【命令】

display qos policy global [**slot** *slot-number*] [**inbound** | **outbound**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

inbound：显示设备所有端口入方向应用的 QoS 策略信息。

outbound：显示设备所有端口出方向应用的 QoS 策略信息。

slot *slot-number*：显示指定成员设备的基于全局应用 QoS 策略的信息。*slot-number* 的取值范围取决于当前 IRF 中的成员数量和编号情况。

|：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 global 命令用来显示基于全局应用 QoS 策略的信息。

需要注意的是：

- 如果不指定显示方向，则同时显示出入两个方向基于全局应用 QoS 策略的信息。
- 如果不指定成员设备，则显示整个 IRF 系统全局应用 QoS 策略的信息。

【举例】

显示基于全局应用 QoS 策略的信息。

```
<Sysname> display qos policy global
```

```
Direction: Inbound

Policy: 1
 Classifier: 2
   Operator: AND
   Rule(s) : If-match acl 2000
   Behavior: 2
     Accounting Enable
       20864 (Bytes)
     Committed Access Rate:
       CIR 128 (kbps), CBS 8000 (Bytes), EBS 0 (Bytes)
       Red Action: discard
       Green : 12928(Bytes)
       Red   : 43904(Bytes)

Direction: Outbound

Policy: 2
 Classifier: 2 (Failed)
   Operator: AND
   Rule(s) : If-match customer-dot1p 3
   Behavior: 1
    Marking:
      Remark local precedence 2
```

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

字段	描述
Direction	对接收到（Inbound）/发送（Outbound）的报文应用QoS策略
Policy	策略名称及其内容
Classifier	类的名称及其内容；如果在类的名称后面显示“(Failed)”，表示该流分类以及与其关联的流行为所组成的关联组没有在全局正常应用； 在IRF中： • 如果在没有使用 **slot** 参数的情况下显示“(Failed)”，表示该关联组没有在 IRF 全局正常应用 • 如果在使用了 **slot** 参数的情况下显示“(Failed)”，表示该关联组没有在指定成员设备的全局正常应用 一个QoS策略中可以存在多个关联组，某个关联组的下发失败并不影响其它关联组的正常应用
Mode	类和流行为的对应关系所支持的模式
Operator	分类规则之间的逻辑关系
Rule(s)	分类规则
Behavior	流行为的名称及其内容，内容可以有多种类型

1.3.4 display qos policy interface

【命令】

display qos policy interface [*interface-type interface-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：指定的端口类型和端口编号。

inbound：显示对端口接收到的报文应用的 QoS 策略信息。

outbound：显示对端口发送的报文应用的 QoS 策略信息。

|：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 命令用来显示指定端口或所有端口上 QoS 策略的配置信息和运行情况。

【举例】

显示 GigabitEthernet1/0/1 端口上 QoS 策略的配置信息和运行情况。

```
<Sysname> display qos policy interface gigabitethernet 1/0/1
  Interface: GigabitEthernet1/0/1
  Direction: Inbound
  Policy: 1
   Classifier: 1
     Operator: AND
     Rule(s) : If-match acl 2000
     Behavior: 1
      Accounting Enable:
      Mirror enable:
        Mirror type: interface
        Mirror destination: GigabitEthernet1/0/2
      Redirect enable:
        Redirect type: cpu
        Redirect destination: cpu
      Marking:
        Remark Customer VLAN ID 100
```

```
Marking:
  Remark dot1p COS 2
Marking:
  Remark IP precedence 3
Marking:
  Remark qos local ID 3
```

表1-7 display qos policy interface 命令显示信息描述表

字段	描述
Interface	端口名，由端口类型和端口编号结合在一起组成。
Direction	Policy应用在端口的方向
Policy	应用到端口上的策略的名字
Classifier	策略里分类规则以及对应的配置信息
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

1.3.5 display qos vlan-policy

【命令】

display qos vlan-policy { **name** *policy-name* | **vlan** [*vlan-id*] } [**slot** *slot-number*] [**inbound** | **outbound**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

name *policy-name*：显示指定策略名称的基于 VLAN 应用 QoS 策略的信息。*policy-name* 表示策略名称，为 1～31 个字符的字符串。

vlan *vlan-id*：显示指定 VLAN 上应用的基于 VLAN 应用 QoS 策略的信息。*vlan-id* 表示应用策略的 VLAN ID。

inbound：显示对 VLAN 接收到的报文应用的 QoS 策略信息。

outbound：显示对 VLAN 发送的报文应用的 QoS 策略信息。

slot *slot-number*：显示指定成员设备上基于 VLAN 应用 QoS 策略的信息。*slot-number* 的取值范围取决于当前 IRF 中的成员数量和编号情况。

|：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 vlan-policy 命令用来显示基于 VLAN 应用 QoS 策略的信息。

需要注意的是：

- 如果不指定显示方向，则同时显示出入两个方向基于 VLAN 应用 QoS 策略的信息。
- 如果不指定成员设备，则显示整个 IRF 系统基于 VLAN 应用 QoS 策略的信息。
- 在VLAN的inbound和outbound方向应用QoS策略时，除不支持在出方向应用流镜像动作外，对其它流行为的支持情况与在端口应用QoS策略时相同，具体请参考 qos apply policy命令中的介绍。

【举例】

显示 IRF 中 6 号成员设备上基于 VLAN 应用的名为 test 的 QoS 策略信息。

```
<Sysname> display qos vlan-policy name test slot 6
  Policy test
    Vlan 200：inbound
    Vlan 300：outbound
```

表1-8 display qos vlan-policy 命令显示信息描述表

字段	描述
Policy	QoS策略名称
Vlan	引用QoS策略的VLAN ID
inbound	对VLAN接收到的报文应用QoS策略
outbound	对VLAN发送的报文应用QoS策略

显示 VLAN 2 的 QoS 策略信息。

```
<Sysname> display qos vlan-policy vlan 2
  Vlan 2

  Direction: Inbound

  Policy: 1
   Classifier: 2
     Operator: AND
     Rule(s) : If-match acl 2000
     Behavior: 2
       Accounting Enable
         163 (Packets)
       Committed Access Rate:
         CIR 128 (kbps), CBS 8000 (byte), EBS 0 (byte)
         Red Action: discard
         Green : 12928(Bytes)
         Red   : 43904(Bytes)
```

表1-9 display qos vlan-policy 命令显示信息描述表

字段	描述
Vlan	引用QoS策略的VLAN ID
Direction	对VLAN接收到（Inbound）/发送（Outbound）的报文应用QoS策略
Classifier	类的名称及其内容；如果在类的名称后面显示“(Failed)”，表示该流分类以及与其关联的流行为所组成的关联组没有在全局正常应用； 在IRF中： • 如果在没有使用 **slot** 参数的情况下显示“(Failed)”，表示该关联组没有在 IRF 上正常应用 • 如果在使用了 **slot** 参数的情况下显示“(Failed)”，表示该关联组没有在指定成员设备上正常应用 一个QoS策略中可以存在多个关联组，某个关联组的下发失败并不影响其它关联组的正常应用
Operator	分类规则之间的逻辑关系
Rule(s)	分类规则
Behavior	流行为的名称及其内容，内容可以有多种类型

1.3.6 qos apply policy

【命令】

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

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

【视图】

二层以太网端口视图/三层以太网端口视图

【缺省级别】

2：系统级

【参数】

inbound：入方向。

outbound：出方向。在控制平面视图下不支持该参数。

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。

【举例】

将策略 USER1 应用到端口 GigabitEthernet1/0/1 的出方向上。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos apply policy USER1 outbound
```

1.3.7 qos apply policy global

【命令】

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

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

【视图】

系统视图

【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。

inbound：对设备所有端口接收到的流量应用 QoS 策略。

outbound：对设备所有端口发送的流量应用 QoS 策略。

【描述】

qos apply policy global 命令用来全局应用 QoS 策略，全局应用的 QoS 策略对全部流量生效。

undo qos apply policy global 命令用来取消全局应用的 QoS 策略。

需要注意的是，在全局inbound和outbound方向应用QoS策略时，除不支持在outbound方向应用流镜像动作外，对其它流行为的支持情况与在端口应用QoS策略时相同，具体请参考 qos apply policy 命令中的介绍。

【举例】

将名为 user1 的策略应用到全局的入方向上。

```
<Sysname> system-view
[Sysname] qos apply policy user1 global inbound
```

1.3.8 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。

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

【举例】

定义一个名为 user1 的策略。

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

1.3.9 qos vlan-policy

【命令】

qos vlan-policy *policy-name* **vlan** *vlan-id-list* { **inbound** | **outbound** }

undo qos vlan-policy [*policy-name*] **vlan** *vlan-id-list* { **inbound** | **outbound** }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

policy-name：策略名称，为 1～31 个字符的字符串。

vlan-id-list：VLAN ID 列表，形式可以是 *vlan-id* **to** *vlan-id*，其中，*vlan-id* 为指定 VLAN 的 ID 号，取值范围为 1～4094。可以输入多个不连续的 VLAN ID，中间以空格隔开。设备最多允许用户同时指定 8 个 VLAN ID。

inbound：对 VLAN 接收到的报文应用 QoS 策略。

outbound：对 VLAN 发送的报文应用 QoS 策略。

【描述】

qos vlan-policy 命令用来在指定 VLAN 上应用 QoS 策略。**undo qos vlan-policy** 命令用来取消指定 VLAN 上应用的 QoS 策略。

【举例】

在 VLAN 200、300、400、500 的入方向上应用 VLAN 策略 test。

```
<Sysname> system-view
[Sysname] qos vlan-policy test vlan 200 300 400 500 inbound
```

1.3.10 reset qos policy global

【命令】

reset qos policy global [**inbound** | **outbound**]

【视图】

用户视图

【缺省级别】

1：监控级

【参数】

inbound：入方向。

outbound：出方向。

【描述】

reset qos policy global 命令用来清除全局应用的 QoS 策略的统计信息。

【举例】

清除全局入方向应用的 QoS 策略的统计信息。

```
<Sysname> reset qos policy global inbound
```

1.3.11 reset qos vlan-policy

【命令】

reset qos vlan-policy [**vlan** *vlan-id*] [**inbound** | **outbound**]

【视图】

用户视图

【缺省级别】

1：监控级

【参数】

vlan-id：VLAN 的 ID 号，取值范围为 1～4094。

inbound：清除 VLAN 接收到的报文应用 QoS 策略的统计信息。

outbound：清除对 VLAN 发送的报文应用 QoS 策略的统计信息。

【描述】

reset qos vlan-policy 命令用来清除 VLAN 应用的 QoS 策略的统计信息。

【举例】

清除 VLAN 2 应用的 QoS 策略的统计信息。

```
<Sysname> reset qos vlan-policy vlan 2
```

2 优先级映射

说明

优先级映射功能中的“接口”包括二层以太网端口、三层以太网端口。三层以太网端口是指被配置为三层模式的以太网端口，有关以太网端口模式切换的操作，请参见“二层技术-以太网交换配置指导”中的“以太网端口配置”。

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 [**dot1p-dp** | **dot1p-lp** | **dscp-dot1p** | **dscp-dp** | **dscp-dscp**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

dot1p-dp：802.1p 优先级到丢弃优先级映射表。

dot1p-lp：802.1p 优先级到本地优先级映射表。

dscp-dot1p：DSCP 到 802.1p 优先级映射表。

dscp-dp：DSCP 到丢弃优先级映射表。

dscp-dscp：DSCP 到 DSCP 映射表。

|：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。

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
```

显示 802.1p 优先级到丢弃优先级映射表的配置信息。

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

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 优先级到丢弃优先级映射表参数，与 802.1p 优先级 4、5 相对应的丢弃优先级为 1。

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

2.1.3 qos map-table

【命令】

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

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

dot1p-dp：802.1p 优先级到丢弃优先级映射表。

dot1p-lp：802.1p 优先级到本地优先级映射表。

dscp-dot1p：DSCP 到 802.1p 优先级映射表。

dscp-dp：DSCP 到丢弃优先级映射表。

dscp-dscp：DSCP 到 DSCP 映射表。

【描述】

qos map-table 命令用来进入指定的优先级映射表视图。

相关配置可参考命令 **display qos map-table**。

【举例】

进入 802.1p 优先级到丢弃优先级映射表视图。

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

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

【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。

【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。

缺省情况下，端口的优先级为 0。

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

对于不带有 802.1Q 标签头的报文，交换机将使用端口的优先级作为该端口接收的报文的 802.1p 优先级，然后根据该优先级查找 802.1p 优先级到本地优先级/丢弃优先级映射表，为报文标记本地优先级/丢弃优先级。

【举例】

配置端口 GigabitEthernet1/0/1 的端口优先级为 2。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] 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】

显示端口 GigabitEthernet 1/0/1 的优先级信任模式配置信息。

```
<Sysname> display qos trust interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
 Port priority information
  Port priority :0
  Port priority trust type : dscp
```

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	优先级信任模式： • dscp 表示信任报文的 DSCP 优先级 • dot1p 表示信任报文的 802.1p 优先级

2.3.2 qos trust

【命令】

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

undo qos trust

【视图】

接口视图

【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。

【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。

缺省情况下，信任模式为信任报文的 802.1p 优先级。

【举例】

在端口 GigabitEthernet1/0/1 上配置优先级信任模式为信任报文的 DSCP 优先级。

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos trust dscp
```

3 流量整形/端口限速

说明

流量整形/端口限速功能中的“接口”包括二层以太网端口和三层以太网端口。三层以太网端口是指被配置为三层模式的以太网端口，有关以太网端口模式切换的操作，请参见“二层技术-以太网交换配置指导”中的“以太网端口配置”。

3.1 流量整形配置命令

3.1.1 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 命令用来显示某个接口或所有接口的流量整形配置情况。

如不指定接口，本命令将显示所有接口的流量整形配置情况。

【举例】

显示所有接口的流量整形配置信息。

```
<Sysname> display qos gts interface
Interface: GigabitEthernet1/0/1
Rule(s): If-match queue 2
 CIR 640 (kbps)
```

表3-1 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

3.1.2 qos gts

【命令】

qos gts { **any** | **queue** *queue-number* } **cir** *committed-information-rate*

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

【视图】

二层以太网端口视图

【缺省级别】

2：系统级

【参数】

any：对所有的数据包进行流量整形。

queue *queue-number*：对指定队列的数据包进行流量整形，*queue-number* 为队列编号，取值范围为 0～7。S5830-106S 交换机不支持该参数。

cir *committed-information-rate*：承诺信息速率，单位为 kbps。*committed-information-rate* 在不同端口上的取值分别为：

- 千兆端口的取值范围为 64～1000000 且必须是 64 的倍数。
- 万兆端口的取值范围为 64～10000000 且必须是 64 的倍数。

【描述】

qos gts 命令用来为某一类别的流或端口下所有流设置整形参数，并开始整形。**undo qos gts** 命令用来取消流量整形配置。

缺省情况下，端口上没有配置整形参数。

【举例】

在端口 GigabitEthernet 1/0/1 上所有发送的报文进行流量整形，当速率大于 640 kbps 时，将超出限制的报文进行缓存。

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos gts any cir 640
```

在端口 GigabitEthernet 1/0/1 上对队列 2 发送报文进行流量整形，当速率大于 640 kbps 时，将超出限制的报文进行缓存。

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] qos gts queue 2 cir 640
```

3.2 端口限速配置命令

3.2.1 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端口限速配置情况。

如不指定接口，本命令将显示所有接口的端口限速配置情况和运行统计信息。

【举例】

显示所有接口的端口限速配置情况。

```
<Sysname> display qos lr interface
Interface: GigabitEthernet1/0/1
Direction: Outbound
 CIR 64000 (kbps),  CBS 4000000 (byte)
```

表3-2 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	指明端口限速的方向
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

3.2.2 qos lr

【命令】

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

undo qos lr outbound

【视图】

接口视图

【缺省级别】

2：系统级

【参数】

inbound：对端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，单位为 kbps：*committed-information-rate* 在不同端口上的取值分别为：

- 千兆端口的取值范围为 64～1000000 且必须是 64 的倍数。
- 万兆端口的取值范围为 64～10000000 且必须是 64 的倍数。

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

- 如果不指定 **cbs** 参数，缺省取值为 62.5ms**committed-information-rate*，但是最大值不能超过 16000000。
- 如果指定 **cbs** 参数，取值范围 4000～1600000。

【描述】

qos lr 命令用来限制端口接收或发送数据的速率。**undo qos lr** 命令用来取消限制。

【举例】

限制端口 GigabitEthernet 1/0/1 发送报文的速率为 640kbps。

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos lr outbound cir 640
```

4 拥塞管理

说明

拥塞管理功能中的“端口”包括二层以太网端口和三层以太网端口。三层以太网端口是指被配置为三层模式的以太网端口，有关以太网端口模式切换的操作，请参见“二层技术-以太网交换配置指导”中的“以太网端口配置”。

4.1 严格优先级队列配置命令

4.1.1 display qos sp

【命令】

display qos sp 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：指定的端口类型和端口编号。

|：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 sp interface 命令用来显示端口的 SP（Strict Priority，严格优先级）队列配置情况。如不指定端口，本命令将显示所有端口的 SP 队列配置情况。

相关配置可参考命令 **qos sp**。

【举例】

显示 GigabitEthernet1/0/1 的严格优先级队列配置情况。

```
<Sysname> display qos sp interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
Output queue:   Strict-priority queue
```

表4-1 display qos sp interface 命令显示信息描述表

字段	描述
Interface	端口名，由端口类型和端口编号结合在一起组成
Output queue	当前出队列类型
Strict-priority queue	采用SP队列进行队列调度

4.1.2 qos sp

【命令】

qos sp

undo qos sp

【视图】

接口视图

【缺省级别】

2：系统级

【参数】

无

【描述】

qos sp 命令用来在端口上配置严格优先队列。**undo qos sp** 命令用来恢复端口上缺省的队列算法。

缺省情况下，所有端口采用 SP 调度算法。

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

【举例】

在端口 GigabitEthernet1/0/1 上应用 SP 队列调度。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos sp
```

4.2 加权轮询队列配置命令

4.2.1 display qos wrr interface

【命令】

display qos wrr 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：指定的端口类型和端口编号。

|：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 wrr interface 命令用来显示端口的 WRR（Weighted Round Robin，加权轮询）队列配置情况。

如不指定端口，本命令将显示所有端口的 WRR 队列配置情况。

相关配置可参考命令 **qos wrr**。

【举例】

显示端口 GigabitEthernet1/0/1 的 WRR 队列配置情况。

```
<Sysname> display qos wrr interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
 Output queue: Weighted round robin queue
Queue ID    Group    Byte-count
-------------------------------------
   0         1        1
   1         sp       N/A
   2         1        3
   3         1        4
   4         1        5
   5         1        6
   6         1        7
   7         1        8
```

表4-2 display qos wrr interface 命令显示信息描述表

字段	描述
Interface	端口名，由端口类型和端口编号结合在一起组成
Output queue	当前出队列类型
Queue ID	队列号
Group	队列所属调度组，1表示队列处于WRR调度组，sp表示队列处于SP调度组
Byte-count	调度时各个队列的权重，N/A表示该队列采用SP调度算法

4.2.2 qos wrr

【命令】

qos wrr [**byte-count** | **weight**]

undo qos wrr

【视图】

接口视图

【缺省级别】

2：系统级

【参数】

byte-count：表示以字节数为调度单位，即按照每次轮询发送的字节数来体现调度权重。如果不指定调度权重，则缺省使用字节数作为调度权重。

weight：表示以报文个数为调度单位，即按照每次轮询发送的报文个数来体现调度权重。目前不支持配置该参数。

【描述】

qos wrr 命令用来配置端口使用 WRR 队列算法进行调度，并指定调度单位。**undo qos wrr** 命令用来将端口的队列调度权重恢复为缺省值。

缺省情况下，端口使用 SP 队列进行调度。

【举例】

在 GigabitEthernet1/0/1 上使能 WRR 队列。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wrr
```

4.2.3 qos wrr byte-count

【命令】

qos wrr *queue-id* **group 1 byte-count** *schedule-value*

undo qos wrr *queue-id* **group 1 byte-count**

【视图】

接口视图

【缺省级别】

2：系统级

【参数】

queue-id：队列序号，取值范围为 0～7。

1：表示该队列属于 group 1，即 WRR 队列组。

byte-count *schedule-value*：配置队列的调度权重，*schedule-value* 的取值范围为 1～15。

【描述】

qos wrr byte-count 命令用来配置 WRR 队列的调度权重(在使用字节数为调度单位时)。**undo qos wrr byte-count** 命令用来将 WRR 队列参数恢复为缺省情况（在使用字节数为调度单位时)。

缺省情况下，在使用字节数为调度单位时，0～7 队列的调度权重分别为 1、2、3、4、5、6、7、8。

需要注意的是，在使用本命令配置 WRR 队列调度权重前，请确认当前端口的 WRR 队列调度是以字节数作为调度单位，以保证调度权重的配置能够正常生效。

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

【举例】

在 GigabitEthernet1/0/1 上应用 WRR 队列，使用字节数为调度单位，并配置队列 0 的调度权重为 10。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wrr byte-count
[Sysname-GigabitEthernet1/0/1] qos wrr 0 group 1 byte-count 10
```

4.2.4 qos wrr group sp

【命令】

qos wrr *queue-id* **group sp**

undo qos wrr *queue-id* **group sp**

【视图】

接口视图

【缺省级别】

2：系统级

【参数】

queue-id：队列序号，取值 0～7。

sp：严格优先级调度算法。

【描述】

qos wrr group sp 命令用来配置端口使用 SP+WRR 队列算法时加入 SP 调度组的队列。**undo qos wrr group sp** 命令用来取消配置。

本系列以太网交换机的端口支持 8 个输出队列，用户可以根据需要配置端口上的部分队列使用 SP 调度算法，部分队列使用 WRR 调度算法。通过将端口上的队列分别加入 SP 调度组和 WRR 调度组（即 group 1)，实现 SP+WRR 的调度功能。在队列调度时，系统会优先保证 SP 调度组内的队列调度，当 SP 调度组内的队列中没有报文发送时，才会调度 WRR 调度组内的队列。SP 调度组内各个队列执行严格优先级调度方式，WRR 调度组内各个队列执行加权轮询调度方式。

此命令需要在端口队列为 WRR 调度模式下使用。SP 组与普通 WRR 优先组不同，加入 SP 组的端口队列采用严格优先级调度算法，不再采用加权轮循调度算法。

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

【举例】

在 GigabitEthernet1/0/1 端口上应用 WRR 队列，并配置队列 0 加入 SP 组进行严格优先级调度。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wrr
[Sysname-GigabitEthernet1/0/1] qos wrr 0 group sp
```

4.3 加权公平队列配置命令

4.3.1 display qos wfq interface

【命令】

display qos wfq 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：指定的端口类型和端口编号。

|：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 wfq interface 命令用来显示端口的 WFQ 配置情况。

如不指定端口，本命令将显示所有端口的 WFQ 配置情况。

相关配置可参考命令 **qos wfq**。

【举例】

显示端口 GigabitEthernet1/0/1 的加权公平队列配置情况。

```
<Sysname> display qos wfq interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
 Output queue: Hardware weighted fair queue
Queue ID        Group           Byte-count      Min-Bandwidth
------------------------------------------------------------------
0                1               1               NA
1                1               1               NA
2                1               1               NA
3                1               1               NA
```

```
4                1                1                NA
5                1                1                NA
6                1                1                NA
7                1                1                NA
```

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

字段	描述
Interface	端口名，由端口类型和端口编号结合在一起组成
Output queue	当前出队列类型
Queue ID	队列号
Group	队列所属调度组，1表示队列处于WFQ调度组，sp表示队列处于SP调度组
Byte-count	表示队列调度权重为字节数，SP调度组的队列此处显示为NA
Min-Bandwidth	队列的最小保证带宽值，NA表示没有配置此内容

4.3.2 qos bandwidth queue

【命令】

qos bandwidth queue *queue-id* **min** *bandwidth-value*

undo qos bandwidth queue *queue-id* [**min** *bandwidth-value*]

【视图】

接口视图

【缺省级别】

2：系统级

【参数】

queue-id：端口队列序号，取值范围为 0～7。

min *bandwidth-value*：最小保证带宽值，单位为 kbps。*bandwidth-value* 的取值范围在不同端口上分别为：

- 千兆端口的取值范围为 8～1000000。
- 万兆端口的取值范围为 8～10000000。

【描述】

qos bandwidth queue 命令用来配置端口队列的最小带宽保证。**undo qos bandwidth queue** 命令用来取消端口队列的最小带宽保证配置。

缺省情况下，没有配置队列的最小带宽保证。

【举例】

在 GigabitEthernet1/0/1 上配置队列 0 的最小保证带宽值为 100kbps。

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wfq
```

```
[Sysname-GigabitEthernet1/0/1] qos bandwidth queue 0 min 100
```

4.3.3 qos wfq

【命令】

qos wfq [**byte-count** | **weight**]

undo qos wfq

【视图】

接口视图

【缺省级别】

2：系统级

【参数】

byte-count：表示按照每次轮询可发送的字节数作为调度权重。

weight：表示按照每次轮询可发送的报文个数作为调度权重。目前不支持配置该参数。

【描述】

qos wfq 命令用来在端口上使能 WFQ 队列，并指明当前 WFQ 队列调度权重的计算方式。**undo qos wfq** 命令用来恢复端口上缺省的队列算法。

缺省情况下，所有端口采用 SP 调度算法。

如果没有指定调度权重，则使用字节数作为调度权重。

【举例】

在端口 GigabitEthernet 1/0/1 上开启 WFQ 调度算法，并使用字节数作为调度权重。

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wfq byte-count
```

4.3.4 qos wfq byte-count

【命令】

qos wfq *queue-id* **group 1 byte-count** *schedule-value*

undo qos wfq *queue-id* **group 1 byte-count**

【视图】

接口视图

【缺省级别】

2：系统级

【参数】

queue-id：队列序号，取值 0～7。

group 1：表示该队列属于 WFQ 调度组。

byte-count *schedule-value*：配置队列的调度权重，取值范围为 1～15。**byte-count** 表示每次轮询可发送的字节数来计算权重。

【描述】

qos wfq byte-count 命令用来配置 WFQ 队列的调度权重(在使用字节数为调度单位时)。**undo qos wfq byte-count** 命令用来将 WFQ 队列参数恢复为缺省情况（在使用字节数为调度单位时)。

缺省情况下，在使用字节数为调度单位时，0～7 队列的调度权重均为 1。

需要注意的是，在使用本命令配置 WFQ 队列调度权重前，请确认当前端口的 WFQ 队列调度是以字节数作为调度单位，以保证调度权重的配置能够正常生效。

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

【举例】

在 GigabitEthernet1/0/1 上应用 WFQ 队列，使用字节数为调度单位，并配置队列 0 的调度权重为 10。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wfq byte-count
[Sysname-GigabitEthernet1/0/1] qos wfq 0 group 1 byte-count 10
```

4.3.5 qos wfq group sp

【命令】

qos wfq *queue-id* **group sp**

undo qos wfq *queue-id* **group sp**

【视图】

接口视图

【缺省级别】

2：系统级

【参数】

queue-id：队列序号，取值 0～7。

sp：严格优先级调度算法。

【描述】

qos wfq group sp 命令用来配置端口使用 SP+WFQ 队列算法时加入 SP 调度组的队列。**undo qos wfq group sp** 命令用来取消配置。

此命令需要在端口队列为 WFQ 调度模式下使用。SP 组与普通 WFQ 优先组不同，加入 SP 组的端口队列采用严格优先级调度算法，不再采用加权轮循调度算法。

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

【举例】

在 GigabitEthernet1/0/1 上应用 WRR 队列，并配置队列 0 加入 SP 组进行严格优先级调度。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wrr
[Sysname-GigabitEthernet1/0/1] qos wrr 0 group sp
```

5 拥塞避免

说明

拥塞避免功能中的“端口”包括二层以太网端口和三层以太网端口。三层以太网端口是指被配置为三层模式的以太网端口，有关以太网端口模式切换的操作，请参见“二层技术-以太网交换配置指导”中的“以太网端口配置”。

5.1 WRED配置命令

5.1.1 display qos wred interface

【命令】

display qos wred 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：指定的端口类型和端口编号。

|：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 wred interface 命令用来显示指定端口或所有端口的 WRED 配置情况。

如果不指定端口，本命令将显示所有端口的 WRED 配置情况。

【举例】

显示端口 GigabitEthernet 1/0/1 的 WRED 配置信息。

```
<Sysname> display qos wred interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
 Current WRED configuration:
 Applied WRED table name: queue-table1
```

5.1.2 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
------------------------------------------------------------------------
 0    10     80    15    10     80    15    10     80    15
 1    10     80    15    10     80    15    10     80    15
 2    10     80    15    10     80    15    10     80    15
 3    10     80    15    10     80    15    10     80    15
 4    10     80    15    10     80    15    10     80    15
 5    10     80    15    10     80    15    10     80    15
 6    10     80    15    10     80    15    10     80    15
 7    10     80    15    10     80    15    10     80    15
```

表5-1 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	队列编号

字段	描述
gmin	绿色报文（丢弃优先级为0）的丢弃队列长度下限
gmax	绿色报文的丢弃队列长度上限
gprob	绿色报文的丢弃概率
ymin	黄色报文（丢弃优先级为1）的丢弃队列长度下限
ymax	黄色报文的丢弃队列长度上限
yprob	黄色报文的丢弃概率
rmin	红色报文（丢弃优先级为2）的丢弃队列长度下限
rmax	红色报文的丢弃队列长度上限
rprob	红色报文的丢弃概率

5.1.3 qos wred apply

【命令】

qos wred apply *table-name*

undo qos wred apply

【视图】

接口视图

【缺省级别】

2：系统级

【参数】

table-name：WRED 全局表的名字。

【描述】

qos wred apply 命令用来在端口上应用 WRED 表。**undo qos wred apply** 用来取消 WRED 表在端口上的应用。

缺省情况下，端口上没有应用 WRED 表。

相关配置可参考命令 **display qos wred interface**、**display qos wred table** 和 **qos wred table**。

【举例】

在端口上 GigabitEthernet 1/0/1 上应用 WRED 表 queue-table1。

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wred apply queue-table1
```

5.1.4 qos wred queue 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】

table-name：WRED 表的名称，为 1～32 个字符的字符串。

【描述】

qos wred queue 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 WRED 表。

缺省情况下，没有创建 WRED 表。

需要注意的是，用户不能删除已经应用的 WRED 表。

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

【举例】

创建 WRED 表 queue-table1。

```
<Sysname> system-view
[Sysname] qos wred queue table queue-table1
[Sysname-wred-table-queue-table1]
```

5.1.5 queue

【命令】

queue *queue-value* [**drop-level** *drop-level*] **low-limit** *low-limit* **high-limit** *high-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，取值范围为 0～7。

drop-level *drop-level*：丢弃级别，取值范围为 0～2。如果没有指定，后续配置的参数对该队列所有丢弃级别的报文都生效。

low-limit *low-limit*：平均队列长度的丢弃下限，取值范围为 0～100，缺省为 10。

high-limit *high-limit*：平均队列长度的丢弃上限，取值范围为 30～100 且必须大于 *low-limit*，缺省为 80。

discard-probability *discard-prob*：以百分数形式表示的丢弃概率，*discard-prob* 的取值范围为 0～100。当报文队列平均长度在上限和下限之间时，设备采用这个概率来丢弃报文。

【描述】

queue 命令用来编辑 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，WRED 表在创建后有缺省的一套参数，其中 *low-limit* 的取值为 10，*high-limit* 的取值为 80，*discard-prob* 的取值为 15。

相关配置可参考命令 **qos wred queue table**。

【举例】

配置全局 WRED 表 queue-table1 中队列 1 丢弃参数：对黄色报文的丢弃下限为 10，丢弃上限为 50，丢弃概率为 30%。

```
<Sysname> system-view
[Sysname] qos wred queue table queue-table1
[Sysname-wred-table-queue-table1] queue 1 drop-level 1 low-limit 10 high-limit 50
discard-probability 30
```