



# H3C S5500-EI-D 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: 6W100-20120225  
产品版本: Release 2210

Copyright © 2012 杭州华三通信技术有限公司及其许可者 版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

H3C、**H3C**、Aolynk、、H<sup>3</sup>Care、、TOP G、、IRF、NetPilot、Neocean、NeoVTL、SecPro、SecPoint、SecEngine、SecPath、Comware、Secware、Storware、NQA、VVG、V<sup>2</sup>G、V<sup>n</sup>G、PSPT、XGbus、N-Bus、TiGem、InnoVision、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 S5500-EI-D 系列以太网交换机命令参考共分为十本手册，主要针对 S5500-EI-D 系列以太网交换机 Release2210 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、应用 ACL 进行报文过滤、配置 QoS 策略，以及配置优先级映射、端口限速、拥塞管理、流量重定向等常用 QoS 技术时所使用的命令。

前言部分包含如下内容：

- [读者对象](#)
- [新增及修改命令说明](#)
- [本书约定](#)
- [资料获取方式](#)
- [技术支持](#)
- [资料意见反馈](#)

## 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

## 新增及修改命令说明

本手册对应 S5500-EI-D 系列交换机的 Release2210 软件版本，该版本与 Release2208 版本相比，新增及修改了部分命令，具体请参见下表。

命令参考	新增及修改命令
ACL命令	<p>新增命令：<b>rule remark</b></p> <p>修改命令：</p> <ul style="list-style-type: none"><li>• <b>rule</b> (IPv6 advanced ACL view)命令新增 <b>routing</b> 和 <b>vpn-instance</b> 参数</li><li>• <b>rule</b> (IPv6 basic ACL view)命令新增 <b>routing</b> 和 <b>vpn-instance</b> 参数</li><li>• ACL 相关命令中 ACL 名称的取值范围扩展为 1~63 个字符的字符串</li></ul>

命令参考		新增及修改命令
QoS命令	QoS策略配置命令	无
	优先级映射配置命令	无
	流量整形/端口限速命令	无
	拥塞管理配置命令	新增命令： <ul style="list-style-type: none"> <li>• qos wfq byte-count</li> <li>• qos wfq group sp</li> </ul> 修改命令： <ul style="list-style-type: none"> <li>• qos wfq 命令增加 byte-count 和 weight 参数</li> </ul>
	拥塞避免配置命令	无
	数据缓冲区配置命令	无

## 本书约定

### 1. 命令行格式约定






格式	意义
<b>粗体</b>	命令行关键字（命令中保持不变、必须照输的部分）采用 <b>加粗</b> 字体表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x   y   ... }	表示从两个或多个选项中选一个。
[ x   y   ... ]	表示从两个或多个选项中选一个或者不选。
{ x   y   ... } *	表示从两个或多个选项中选多个，最少选一个，最多选所有选项。
[ x   y   ... ] *	表示从两个或多个选项中选多个或者不选。
&<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。

### 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](http://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](mailto:service@h3c.com)

技术支持热线电话：400-810-0504（手机、固话均可拨打）

010-62982107

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](mailto:info@h3c.com)

感谢您的反馈, 让我们做得更好!

# 目 录

1 ACL配置命令 .....	1-1
1.1 ACL配置命令 .....	1-1
1.1.1 acl .....	1-1
1.1.2 acl copy .....	1-2
1.1.3 acl ipv6 .....	1-3
1.1.4 acl ipv6 copy .....	1-4
1.1.5 acl ipv6 logging frequency .....	1-5
1.1.6 acl ipv6 name .....	1-5
1.1.7 acl logging frequency .....	1-6
1.1.8 acl name .....	1-6
1.1.9 description .....	1-7
1.1.10 display acl .....	1-7
1.1.11 display acl ipv6 .....	1-9
1.1.12 display acl resource .....	1-10
1.1.13 display packet-filter .....	1-11
1.1.14 display time-range .....	1-13
1.1.15 hardware-count enable .....	1-14
1.1.16 packet-filter .....	1-14
1.1.17 packet-filter ipv6 .....	1-15
1.1.18 reset acl counter .....	1-16
1.1.19 reset acl ipv6 counter .....	1-16
1.1.20 rule (Ethernet frame header ACL view) .....	1-17
1.1.21 rule (IPv4 advanced ACL view) .....	1-18
1.1.22 rule (IPv4 basic ACL view) .....	1-22
1.1.23 rule (IPv6 advanced ACL view) .....	1-24
1.1.24 rule (IPv6 basic ACL view) .....	1-28
1.1.25 rule comment .....	1-30
1.1.26 rule remark .....	1-30
1.1.27 step .....	1-32
1.1.28 time-range .....	1-32

# 1 ACL配置命令

---



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**: 指定所有的 IPv4 ACL 及二层 ACL。

#### 【描述】

**acl** 命令用来创建一个 IPv4 ACL 或二层 ACL，并进入相应的 ACL 视图。**undo acl** 命令用来删除 IPv4 ACL 或二层 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**。若未指定本参数，系统将不会为目的 ACL 设置名称。

### 【描述】

**acl copy** 命令用来复制生成一个新的同类型 IPv4 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 IPv4 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 IPv6 ACL 的编号。*acl6-number* 表示 IPv6 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 IPv6 ACL 的名称。*acl6-name* 表示 IPv6 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**: 指定所有的 IPv6 ACL。

### 【描述】

**acl ipv6** 命令用来创建一个 IPv6 ACL，并进入相应的 ACL 视图。**undo acl ipv6** 命令用来删除 IPv6 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 IPv6 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 IPv6 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 IPv6 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 IPv6 ACL 的编号，该 ACL 必须不存在。若未指定本参数，系统将为目的 IPv6 ACL 自动分配一个与源 IPv6 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 IPv6 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 IPv6 ACL 设置名称。

#### 【描述】

**acl ipv6 copy** 命令用来复制生成一个新的同类型 IPv6 ACL。

需要注意的是：

- 目的 IPv6 ACL 的类型要与源 IPv6 ACL 的类型相同。
- 目的 IPv6 ACL 的名称只能在复制时设置。目的 IPv6 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 IPv6 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 IPv6 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 IPv6 ACL。

```
<Sysname> system-view
[Sysname] acl ipv6 copy 2001 to 2002
```

## 1.1.5 acl ipv6 logging frequency

### 【命令】

```
acl ipv6 logging frequency frequency  
undo acl ipv6 logging frequency
```

### 【视图】

系统视图

### 【缺省级别】

2: 系统级

### 【参数】

**frequency**: 指定 IPv6 报文过滤日志的生成与发送周期，取值范围为 0~1440，且必须为 5 的整数倍，0 表示不记录，单位为分钟。

### 【描述】

**acl ipv6 logging frequency** 命令用来配置 IPv6 报文过滤日志的生成与发送周期，设备将周期性地生成并发送报文过滤的日志信息，包括该周期内被匹配的报文数量以及所使用的 IPv6 ACL 规则。

**undo acl ipv6 logging frequency** 命令用来恢复缺省情况。

缺省情况下，IPv6 报文过滤日志的生成与发送周期为 0 分钟，即不记录 IPv6 报文过滤的日志。

需要注意的是，系统只支持对应用 IPv6 基本或高级 ACL 进行报文过滤的日志进行记录，且在上述 ACL 中配置规则时须指定 **logging** 参数。

相关配置可参考命令 **packet-filter ipv6**、**rule** (IPv6 advanced ACL view)和 **rule** (IPv6 basic ACL view)。

### 【举例】

# 配置 IPv6 报文过滤日志的生成与发送周期为 10 分钟。

```
<Sysname> system-view  
[Sysname] acl ipv6 logging frequency 10
```

## 1.1.6 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 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 ACL 视图。

相关配置可参考命令 **acl ipv6**。

### 【举例】

# 进入名称为 flow 的 IPv6 ACL 的视图。

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

```
[Sysname] acl ipv6 name flow
[Sysname-acl6-basic-2001-flow]
```

### 1.1.7 acl logging frequency

#### 【命令】

```
acl logging frequency frequency
undo acl logging frequency
```

#### 【视图】

系统视图

#### 【缺省级别】

2: 系统级

#### 【参数】

**frequency**: 指定 IPv4 报文过滤日志的生成与发送周期，取值范围为 0~1440，且必须为 5 的整数倍，0 表示不进行记录，单位为分钟。

#### 【描述】

**acl logging frequency** 命令用来配置 IPv4 报文过滤日志的生成与发送周期，设备将周期性地生成并发送报文过滤的日志信息，包括该周期内被匹配的报文数量以及所使用的 IPv4 ACL 规则。**undo acl logging frequency** 命令用来恢复缺省情况。

缺省情况下，IPv4 报文过滤日志的生成与发送周期为 0 分钟，即不记录 IPv4 报文过滤的日志。

需要注意的是，系统只支持对应用 IPv4 基本或高级 ACL 进行报文过滤的日志进行记录，且在上述 ACL 中配置规则时须指定 **logging** 参数。

相关配置可参考命令 **packet-filter**、**rule** (IPv4 advanced ACL view)和 **rule** (IPv4 basic ACL view)。

#### 【举例】

# 配置 IPv4 报文过滤日志的生成与发送周期为 10 分钟。

```
<Sysname> system-view
[Sysname] acl logging frequency 10
```

### 1.1.8 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 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 ACL 视图。

相关配置可参考命令 **acl**。

#### 【举例】

# 进入名称为 flow 的 IPv4 ACL 的视图。

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

### 1.1.9 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.
```

### 1.1.10 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 IPv4 ACL 的配置和运行情况。*acl-number* 表示 IPv4 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:** 显示所有 IPv4 ACL 的配置和运行情况。

**name acl-name:** 显示指定名称的 IPv4 ACL 的配置和运行情况。*acl-name* 表示 IPv4 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 IRF 中指定成员设备的 IPv4 ACL 运行情况, *slot-number* 表示成员设备编号, 取值范围取决于当前 IRF 中的成员数量和编号情况。如未指定 **slot slot-number** 参数, 在 IRF 环境中将显示 IRF 中所有设备的 IPv4 ACL 运行情况。

**|:** 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 IPv4 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】

# 显示所有 IPv4 ACL 的配置和运行情况。

```
<Sysname> display acl all
Basic ACL 2000, named flow, 3 rules,
Statistics is enabled
ACL's step is 5
rule 0 permit
rule 5 permit source 1.1.1.1 0 (5 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 source 1.1.1.1 0
rule 10 comment This rule is used in 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: <ul style="list-style-type: none"> <li>• Basic ACL: 表示 IPv4 基本 ACL</li> <li>• Advanced ACL: 表示 IPv4 高级 ACL</li> <li>• Ethernet frame ACL: 表示二层 ACL</li> </ul>
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)
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



字段	描述
rule 0 permit	规则 0 的具体内容
5 times matched	该规则匹配的次数为 5，在 ACL 规则中未配置 <b>counting</b> 参数且在 ACL 视图下未配置 <b>hardware-count enable</b> 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 <b>counting</b> 参数或 <b>hardware-count enable</b> 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 rd.	规则 10 的描述信息为 This rule is used in rd.

### 1.1.11 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 IPv6 ACL 的配置和运行情况。**acl6-number** 表示 IPv6 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**: 显示所有 IPv6 ACL 的配置和运行情况。

**name acl6-name**: 显示指定名称的 IPv6 ACL 的配置和运行情况。**acl6-name** 表示 IPv6 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 IRF 中指定成员设备的 IPv6 ACL 运行情况，**slot-number** 表示成员设备编号，取值范围取决于当前 IRF 中的成员数量和编号情况。如未指定 **slot slot-number** 参数，在 IRF 环境中将显示 IRF 中所有设备的 IPv6 ACL 运行情况。

|: 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 IPv6 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】

# 显示所有 IPv6 ACL 的配置和运行情况。



```

<Sysname> display acl ipv6 all
Basic IPv6 ACL 2000, named flow, 3 rules,
Statistics is enabled
ACL's step is 5
rule 0 permit
rule 5 permit source 1::/64 (5 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 source 1::/64
rule 10 comment This rule is used in rd.
rule 5 permit source 2::/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： <ul style="list-style-type: none"> <li>Basic IPv6 ACL：表示 IPv6 基本 ACL</li> <li>Advanced IPv6 ACL：表示 IPv6 高级 ACL</li> </ul>
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）
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
5 times matched	该规则匹配的次数为 5，在 ACL 规则中未配置 <b>counting</b> 参数且在 ACL 视图下未配置 <b>hardware-count enable</b> 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 <b>counting</b> 参数或 <b>hardware-count enable</b> 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 rd.	规则 10 的描述信息为 This rule is used in rd.

### 1.1.12 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 IRF 中指定设备的 ACL 资源的使用情况，*slot-number* 的取值范围取决于当前 IRF 中的成员数量和编号情况。如未指定 **slot slot-number** 参数，在 IRF 环境中将显示 IRF 中所有成员设备 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 ACL 资源的使用情况。

```
<H3C>display acl resource
Interface:
  GE2/0/1 to GE2/0/28, XGE2/2/1 to XGE2/2/2
```

Type	Total	Reserved	Configured	Remaining	Usage
VFP ACL	1024	0	0	1024	0%
IFP ACL	4096	1536	0	2560	37%
IFP Meter	2048	768	0	1280	37%
IFP Counter	2048	768	0	1280	37%
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
Type	资源类型： <ul style="list-style-type: none"> <li>• ACL 表示 ACL 规则资源</li> <li>• Meter 表示流量监管资源</li> <li>• Counter 表示流量统计资源</li> <li>• VFP 表示二层转发前的，应用于 QinQ 功能的资源数目</li> <li>• IFP 表示入方向的资源数目</li> <li>• EFP 表示出方向的资源数目</li> </ul>
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

## 1.1.13 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**: 显示所有接口上报文过滤策略的应用情况。

**interface interface-type interface-number**: 显示指定接口上报文过滤策略的应用情况。  
*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**: 显示接口入方向上报文过滤策略的应用情况。

**outbound**: 显示接口出方向上报文过滤策略的应用情况。

**interface vlan-interface vlan-interface-number**: 显示指定 VLAN 接口上报文过滤策略的应用情况。  
*vlan-interface-number* 表示 VLAN 接口的编号。

**slot slot-number**: 显示 IRF 中指定成员设备的 VLAN 接口上报文过滤策略的应用情况。*slot-number* 表示成员设备编号，取值范围取决于当前 IRF 中的成员数量和编号情况。如果不指定该参数，将显示 IRF 中 Master 设备的 VLAN 接口上报文过滤策略应用情况。

**|**: 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** 命令用来显示报文过滤策略的应用情况。

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】

# 显示端口 GigabitEthernet1/0/1 出、入方向上报文过滤策略的应用情况。

```
<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	应用报文过滤策略的接口名称
In-bound Policy	入方向报文过滤策略的应用情况
Out-bound Policy	出方向报文过滤策略的应用情况

字段	描述
acl 2001, Successful	应用 IPv4 ACL 2001 成功
acl6 2500, Fail	应用 IPv6 ACL 2500 失败

### 1.1.14 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 23:59 1/31/2010
  from 00:00 6/1/2010 to 23:59 6/30/2010
```

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： <ul style="list-style-type: none"> <li>• 时间段的名称</li> <li>• 时间段的状态，包括 Active（生效）和 Inactive（未生效）两种状态</li> <li>• 时间段的时间范围</li> </ul>

### 1.1.15 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 的基于硬件应用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 的基于硬件应用的规则匹配统计功能。

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

### 1.1.16 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 IPv4 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 IPv4 ACL 的名称。**acl-name** 表示 IPv4 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 IPv4 基本 ACL、IPv4 高级 ACL 或二层 ACL 进行报文过滤。

**undo packet-filter** 命令用来恢复缺省情况。

缺省情况下，接口不对报文进行过滤。

相关配置可参考命令 **display packet-filter**。

## 【举例】

# 应用 IPv4 ACL 2001 对端口 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
```

### 1.1.17 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 IPv6 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 IPv6 ACL 的名称。**acl6-name** 表示 IPv6 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 IPv6 基本 ACL 或 IPv6 高级 ACL 进行报文过滤。**undo packet-filter ipv6** 命令用来恢复缺省情况。

缺省情况下，接口不对报文进行过滤。

相关配置可参考命令 **display packet-filter**。

## 【举例】

```
# 应用 IPv6 ACL 2500 对端口 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
```

### 1.1.18 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**: 指定所有的 IPv4 ACL。

**name acl-name**: 指定 IPv4 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 IPv4 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
```

# 清除名为 flow 的 IPv4 ACL 的统计信息。

```
<Sysname> reset acl counter name flow
```

### 1.1.19 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 IPv6 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**: 指定所有的 IPv6 ACL。

**name acl6-name:** 指定 IPv6 ACL 的名称。*acl6-name* 表示 IPv6 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 IPv6 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
```

# 清除名为 flow 的 IPv6 ACL 的统计信息。

```
<Sysname> reset acl ipv6 counter name flow
```

### 1.1.20 rule (Ethernet frame header ACL view)

#### 【命令】

```
rule [ rule-id ] { deny | permit } [ cos vlan-pri | counting | dest-mac dest-addr dest-mask | { lsap lsap-type lsap-type-mask | type protocol-type protocol-type-mask } | source-mac sour-addr 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。

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

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

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

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



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

### 【描述】

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

缺省情况下，二层 ACL 内不存在任何规则。

需要注意的是：

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

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



### 说明

需要注意的是，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 将无法正常使用。

### 【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
```

#### 1.1.21 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-addr dest-wildcard | any } | destination-port operator port1 [ port2 ] | dscp dscp | fragment | icmp-type { icmp-type [ icmp-code ] | icmp-message } | logging | precedence precedence | source { sour-addr sour-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
<b>source</b> { <i>sour-addr</i> <i>sour-wildcard</i>   <b>any</b> }	源地址	指定 ACL 规则的源地址信息	<i>sour-addr sour-wildcard</i> : 源 IP 地址及其通配符掩码 (为 0 表示主机地址) <b>any</b> : 任意源 IP 地址
<b>destination</b> { <i>dest-addr</i> <i>dest-wildcard</i>   <b>any</b> }	目的地址	指定 ACL 规则的目的地址信息	<i>dest-addr dest-wildcard</i> : 目的 IP 地址及其通配符掩码 (为 0 表示主机地址) <b>any</b> : 任意目的 IP 地址
<b>counting</b>	统计	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 中某条规则的匹配次数
<b>precedence</b> <i>precedence</i>	报文优先级	IP 优先级	<i>precedence</i> : 用数字表示时, 取值范围为 0~7; 用名称表示时, 为 <b>routine</b> 、 <b>priority</b> 、 <b>immediate</b> 、 <b>flash</b> 、 <b>flash-override</b> 、 <b>critical</b> 、 <b>internet</b> 或 <b>network</b> , 分别对应于数字 0~7
<b>tos tos</b>	报文优先级	ToS 优先级	<i>tos</i> : 用数字表示时, 取值范围为 0~15; 用名称表示时, 可选取 <b>max-reliability</b> (2)、 <b>max-throughput</b> (4)、 <b>min-delay</b> (8)、 <b>min-monetary-cost</b> (1) 或 <b>normal</b> (0)
<b>dscp dscp</b>	报文优先级	DSCP 优先级	<i>dscp</i> : 用数字表示时, 取值范围为 0~63; 用名称表示时, 可选取 <b>af11</b> (10)、 <b>af12</b> (12)、 <b>af13</b> (14)、 <b>af21</b> (18)、 <b>af22</b> (20)、 <b>af23</b> (22)、 <b>af31</b> (26)、 <b>af32</b> (28)、 <b>af33</b> (30)、 <b>af41</b> (34)、 <b>af42</b> (36)、 <b>af43</b> (38)、 <b>cs1</b> (8)、 <b>cs2</b> (16)、 <b>cs3</b> (24)、 <b>cs4</b> (32)、 <b>cs5</b> (40)、 <b>cs6</b> (48)、 <b>cs7</b> (56)、 <b>default</b> (0) 或 <b>ef</b> (46)
<b>logging</b>	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, 例如报文过滤
<b>vpn-instance</b> <i>vpn-instance-name</i>	VPN 实例	对指定 VPN 实例中的报文有效	<i>vpn-instance-name</i> : 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

参数	类别	作用	说明
<b>fragment</b>	报文分片	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
<b>time-range</b> <i>time-range-name</i>	时间段	指定规则生效的时间段	<b>time-range-name</b> : 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
<b>source-port</b> <i>operator port1</i> [ <i>port2</i> ]	源端口	定义 TCP/UDP 报文的源端口信息	<b>operator</b> : 操作符，取值可以为 <b>lt</b> (小于)、 <b>gt</b> (大于)、 <b>eq</b> (等于)、 <b>neq</b> (不等于) 或者 <b>range</b> (在范围内，包括边界值)。只有 <b>range</b> 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 <b>port1/port2</b> : 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 <b>chargen</b> (19)、 <b>bgp</b> (179)、 <b>cmd</b> (514)、 <b>daytime</b> (13)、 <b>discard</b> (9)、 <b>domain</b> (53)、 <b>echo</b> (7)、 <b>exec</b> (512)、 <b>finger</b> (79)、 <b>ftp</b> (21)、 <b>ftp-data</b> (20)、 <b>gopher</b> (70)、 <b>hostname</b> (101)、 <b>irc</b> (194)、 <b>klogin</b> (543)、 <b>kshell</b> (544)、 <b>login</b> (513)、 <b>lpd</b> (515)、 <b>nntp</b> (119)、 <b>pop2</b> (109)、 <b>pop3</b> (110)、 <b>smtp</b> (25)、 <b>sunrpc</b> (111)、 <b>tacacs</b> (49)、 <b>talk</b> (517)、 <b>telnet</b> (23)、 <b>time</b> (37)、 <b>uucp</b> (540)、 <b>whois</b> (43) 或 <b>www</b> (80)；UDP 端口号可选取 <b>biff</b> (512)、 <b>bootpc</b> (68)、 <b>bootps</b> (67)、 <b>discard</b> (9)、 <b>dns</b> (53)、 <b>dnsix</b> (90)、 <b>echo</b> (7)、 <b>moblip-ag</b> (434)、 <b>moblip-mn</b> (435)、 <b>nameserver</b> (42)、 <b>netbios-dgm</b> (138)、 <b>netbios-ns</b> (137)、 <b>netbios-ssn</b> (139)、 <b>ntp</b> (123)、 <b>rip</b> (520)、 <b>snmp</b> (161)、 <b>snmptrap</b> (162)、 <b>sunrpc</b> (111)、 <b>syslog</b> (514)、 <b>tacacs-ds</b> (65)、 <b>talk</b> (517)、 <b>tftp</b> (69)、 <b>time</b> (37)、 <b>who</b> (513) 或 <b>xmcp</b> (177)
{ <b>ack</b> <i>ack-value</i>   <b>fin</b> <i>fin-value</i>   <b>psh</b> <i>psh-value</i>   <b>rst</b> <i>rst-value</i>   <b>syn</b> <i>syn-value</i>   <b>urg</b> <i>urg-value</i> }*	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 <i>value</i> 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”
<b>established</b>	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
<b>icmp-type</b> { <i>icmp-type</i> [ <i>icmp-code</i> ]   <i>icmp-message</i> }	ICMP 报文的消 息类型和消息码	指定规则的 ICMP 报文的消 息类型和消息码 信息	<i>icmp-type</i> : ICMP 消息类型, 取值范围为 0~255 <i>icmp-code</i> : ICMP 消息码, 取值范围为 0~255 <i>icmp-message</i> : 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 <a href="#">表 1-9</a> 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，并对符合此条件的行为记录日志。

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

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

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

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

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

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

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

### 1.1.22 rule (IPv4 basic ACL view)

#### 【命令】

```
rule [ rule-id ] { deny | permit } [ counting | fragment | logging | source { sour-addr sour-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，例如报文过滤。

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

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

**vpn-instance vpn-instance-name**: 表示对指定 VPN 实例中的报文有效。*vpn-instance-name* 表示 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 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
```

### 1.1.23 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
dest-prefix | dest/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 source-prefix | source/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 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
<b>source</b> { <i>source</i> <i>source-prefix</i>   <i>source/source-prefix</i>   <b>any</b> }	源 IPv6 地址	指定 IPv6 ACL 规则的源 IPv6 地址信息	<b>source</b> : 源 IPv6 地址 <b>source-prefix</b> : 前缀长度, 取值范围 1~128 <b>any</b> : 任意源 IPv6 地址
<b>destination</b> { <i>dest</i> <i>dest-prefix</i>   <i>dest/dest-prefix</i>   <b>any</b> }	目的 IPv6 地址	指定 IPv6 ACL 规则的目 的 IPv6 地址信息	<b>dest</b> : 目的 IPv6 地址 <b>dest-prefix</b> : 前缀长度, 取值范围 1~128 <b>any</b> : 任意目的 IPv6 地址
<b>counting</b>	统计	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 中 某条规则的匹配次数
<b>dscp</b> <i>dscp</i>	报文优先级	DSCP 优先级	<b>dscp</b> : 用数字表示时, 取值范围为 0~63; 用名称表示时, 可选取 <b>af11</b> (10)、 <b>af12</b> (12)、 <b>af13</b> (14)、 <b>af21</b> (18)、 <b>af22</b> (20)、 <b>af23</b> (22)、 <b>af31</b> (26)、 <b>af32</b> (28)、 <b>af33</b> (30)、 <b>af41</b> (34)、 <b>af42</b> (36)、 <b>af43</b> (38)、 <b>cs1</b> (8)、 <b>cs2</b> (16)、 <b>cs3</b> (24)、 <b>cs4</b> (32)、 <b>cs5</b> (40)、 <b>cs6</b> (48)、 <b>cs7</b> (56)、 <b>default</b> (0) 或 <b>ef</b> (46)
<b>flow-label</b> <i>flow-label-value</i>	流标签字段	指定 IPv6 基本报文中 流标签字段的值	<b>flow-label-value</b> : 流标签字段的值, 取值 范围为 0~1048575
<b>logging</b>	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, 例如报文过滤
<b>routing</b> [ <b>type</b> <i>routing-type</i> ]	路由头	指定路由头的类型	<b>routing-type</b> : 路由头类型的值, 取值范围 为 0~255 若指定了 <b>type routing-type</b> 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
<b>vpn-instance</b> <i>vpn-instance-name</i>	VPN 实例	对指定 VPN 实例中的报 文有效	<b>vpn-instance-name</b> : 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
<b>fragment</b>	报文分片	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
<b>time-range</b> <i>time-range-name</i>	时间段	指定规则生效的时间段	<b>time-range-name</b> : 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
<b>source-port</b> <i>operator port1</i> [ <i>port2</i> ]	源端口	定义 TCP/UDP 报文的源端口信息	<i>operator</i> : 操作符, 取值可以为 <b>lt</b> (小于)、 <b>gt</b> (大于)、 <b>eq</b> (等于)、 <b>neq</b> (不等于) 或者 <b>range</b> (在范围内, 包括边界值)。只有 <b>range</b> 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 <i>port1/port2</i> : 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 <b>chargen</b> (19)、 <b>bgp</b> (179)、 <b>cmd</b> (514)、 <b>daytime</b> (13)、 <b>discard</b> (9)、 <b>domain</b> (53)、 <b>echo</b> (7)、 <b>exec</b> (512)、 <b>finger</b> (79)、 <b>ftp</b> (21)、 <b>ftp-data</b> (20)、 <b>gopher</b> (70)、 <b>hostname</b> (101)、 <b>irc</b> (194)、 <b>klogin</b> (543)、 <b>kshell</b> (544)、 <b>login</b> (513)、 <b>lpd</b> (515)、 <b>nntp</b> (119)、 <b>pop2</b> (109)、 <b>pop3</b> (110)、 <b>smtp</b> (25)、 <b>sunrpc</b> (111)、 <b>tacacs</b> (49)、 <b>talk</b> (517)、 <b>telnet</b> (23)、 <b>time</b> (37)、 <b>uucp</b> (540)、 <b>whois</b> (43) 或 <b>www</b> (80); UDP 端口号可选取 <b>biff</b> (512)、 <b>bootpc</b> (68)、 <b>bootps</b> (67)、 <b>discard</b> (9)、 <b>dns</b> (53)、 <b>dnsix</b> (90)、 <b>echo</b> (7)、 <b>moblip-ag</b> (434)、 <b>moblip-mn</b> (435)、 <b>nameserver</b> (42)、 <b>netbios-dgm</b> (138)、 <b>netbios-ns</b> (137)、 <b>netbios-ssn</b> (139)、 <b>ntp</b> (123)、 <b>rip</b> (520)、 <b>snmp</b> (161)、 <b>snmptrap</b> (162)、 <b>sunrpc</b> (111)、 <b>syslog</b> (514)、 <b>tacacs-ds</b> (65)、 <b>talk</b> (517)、 <b>tftp</b> (69)、 <b>time</b> (37)、 <b>who</b> (513) 或 <b>xdmcp</b> (177)
<b>destination-port</b> <i>operator port1</i> [ <i>port2</i> ]	目的端口	定义 TCP/UDP 报文的端口信息	
{ <b>ack</b> <i>ack-value</i>   <b>fin</b> <i>fin-value</i>   <b>psh</b> <i>psh-value</i>   <b>rst</b> <i>rst-value</i>   <b>syn</b> <i>syn-value</i>   <b>urg</b> <i>urg-value</i> } *	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 <i>value</i> 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”
<b>established</b>	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
<b>icmp6-type</b> { <i>icmp6-type</i> <i>icmp6-code</i>   <i>icmp6-message</i> }	ICMPv6 报文的 消息类型和 消息码	指定规则的 ICMPv6 报文的 消息类型和 消息码信息	<i>icmp6-type</i> : ICMPv6 消息类型, 取值范围为 0~255 <i>icmp6-code</i> : ICMPv6 消息码, 取值范围为 0~255 <i>icmp6-message</i> : 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 <a href="#">表 1-13</a> 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

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

### 【描述】

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

缺省情况下，IPv6 高级 ACL 内不存在任何规则。

需要注意的是：

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

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



### 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**、**routing** 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，并对符合此条件的行为记录日志。

```

<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule permit tcp source 2030:5060::/64 destination fe80:5060::/96
destination-port eq 80 logging
# 为 IPv6 高级 ACL 3001 创建规则如下：允许 IPv6 报文通过，但拒绝发往 FE80:5060:1001::/48
网段的 ICMPv6 报文通过。
<Sysname> system-view
[Sysname] acl ipv6 number 3001
[Sysname-acl6-adv-3001] rule permit ipv6
[Sysname-acl6-adv-3001] rule deny icmpv6 destination fe80:5060:1001:: 48
# 为 IPv6 高级 ACL 3002 创建规则如下：在出、入双方向上都允许建立 FTP 连接并传输 FTP 数据。
<Sysname> system-view
[Sysname] acl ipv6 number 3002
[Sysname-acl6-adv-3002] rule permit tcp source-port eq ftp
[Sysname-acl6-adv-3002] rule permit tcp source-port eq ftp-data
[Sysname-acl6-adv-3002] rule permit tcp destination-port eq ftp
[Sysname-acl6-adv-3002] rule permit tcp destination-port eq ftp-data
# 为 IPv6 高级 ACL 3003 创建规则如下：在出、入双方向上都允许 SNMP 报文和 SNMP Trap 报文
通过。
<Sysname> system-view
[Sysname] acl ipv6 number 3003
[Sysname-acl6-adv-3003] rule permit udp source-port eq snmp
[Sysname-acl6-adv-3003] rule permit udp source-port eq snmptrap
[Sysname-acl6-adv-3003] rule permit udp destination-port eq snmp
[Sysname-acl6-adv-3003] rule permit udp destination-port eq snmptrap

```

## 1.1.24 rule (IPv6 basic ACL view)

### 【命令】

```

rule [ rule-id ] { deny | permit } [ counting | fragment | logging | routing [ type routing-type ] |
source { ipv6-address prefix-length | ipv6-address/prefix-length | 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 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，例如报文过滤。

**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 { ipv6-address prefix-length | ipv6-address/prefix-length | any }:** 指定规则的源 IPv6 地址信息。*ipv6-address* 表示报文的源 IPv6 地址，*prefix-length* 表示源 IPv6 地址前缀长度，取值范围为 1~128。**any** 表示任意源 IPv6 地址。

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

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

### 【描述】

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

缺省情况下，IPv6 基本 ACL 内不存在任何规则。

需要注意的是：

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

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



### 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
```

## 1.1.25 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.
```

## 1.1.26 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，可以是尚不存在规则的编号，也可以是已存在规则的编号，取值范围为 0~65534。该编号用来确定注释信息显示的位置，即使采用了已存在规则的编号，也不会对该规则产生任何影响。

**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** 命令时通过指定 *rule-id* 参数，可以确定注释信息的显示位置：如果指定的编号小于等于现有某条规则的编号，该注释信息将出现在该规则之前；否则，就会出现在该规则之后。
- 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* 参数，将删除所有规则注释信息。
- 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
```

# 为规则编号为 10~25 的四条规则配置如下注释信息：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。

### 1.1.27 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
```

### 1.1.28 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*: 表示周期时间段的时间范围。*start-time* 和 *end-time* 分别表示起始时间和结束时间，格式均为 hh:mm，hh 的取值范围为 0~23，mm 的取值范围为 0~59，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, hh 的取值范围为 0~23, mm 的取值范围为 0~59。**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, hh 的取值范围为 0~24, mm 的取值范围为 0~59。**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 **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。
- 用户使用同一名称可以配置内容不同的多条时间段, 所配置的各周期时间段之间以及各绝对时间段之间分别取并集之后, 各并集的交集将成为最终生效的时间范围。
- 用户最多可以创建 256 个不同名称的时间段, 同一名称下最多可以配置 32 条周期时间段和 12 条绝对时间段。

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 23:59 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 23:59 12/31/2010
```



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

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

```
[Sysname] time-range t4 10:0 to 12:0 1 from 0:0 1/1/2010 to 23:59 1/31/2010
```

```
[Sysname] time-range t4 14:0 to 16:0 3 from 0:0 6/1/2010 to 23:59 6/30/2010
```

# 目 录

1 QoS策略配置命令 .....	1-1
1.1 定义类的命令 .....	1-1
1.1.1 display traffic classifier .....	1-1
1.1.2 if-match .....	1-2
1.1.3 traffic classifier .....	1-6
1.2 定义流行为的命令 .....	1-6
1.2.1 accounting .....	1-6
1.2.2 car .....	1-7
1.2.3 display traffic behavior .....	1-8
1.2.4 filter .....	1-9
1.2.5 redirect .....	1-9
1.2.6 remark dot1p .....	1-10
1.2.7 remark drop-precedence .....	1-11
1.2.8 remark dscp .....	1-11
1.2.9 remark ip-precedence .....	1-13
1.2.10 remark local-precedence .....	1-13
1.2.11 traffic behavior .....	1-14
1.3 定义策略和应用策略的命令 .....	1-14
1.3.1 classifier behavior .....	1-14
1.3.2 control-plane .....	1-15
1.3.3 display qos policy .....	1-15
1.3.4 display qos policy control-plane .....	1-16
1.3.5 display qos policy control-plane pre-defined .....	1-18
1.3.6 display qos policy global .....	1-19
1.3.7 display qos policy interface .....	1-21
1.3.8 display qos vlan-policy .....	1-22
1.3.9 qos apply policy (interface view, port group view, control plane view) .....	1-24
1.3.10 qos apply policy (user-profile view) .....	1-24
1.3.11 qos apply policy global .....	1-25
1.3.12 qos policy .....	1-26
1.3.13 qos vlan-policy .....	1-26
1.3.14 reset qos policy control-plane .....	1-27
1.3.15 reset qos policy global .....	1-27
1.3.16 reset qos vlan-policy .....	1-27
2 优先级映射配置命令 .....	2-1
2.1 优先级映射表配置命令 .....	2-1
2.1.1 display qos map-table .....	2-1

2.1.2 import.....	2-2
2.1.3 qos map-table.....	2-3
2.2 端口优先级配置命令.....	2-3
2.2.1 qos priority.....	2-3
2.3 端口优先级信任模式配置命令.....	2-4
2.3.1 display qos trust interface.....	2-4
2.3.2 qos trust.....	2-5
3 流量整形/端口限速命令.....	3-1
3.1 流量整形配置命令.....	3-1
3.1.1 display qos gts interface.....	3-1
3.1.2 qos gts.....	3-2
3.2 端口限速配置命令.....	3-2
3.2.1 display qos lr interface.....	3-2
3.2.2 qos lr.....	3-3
4 拥塞管理配置命令.....	4-1
4.1 严格优先级队列配置命令.....	4-1
4.1.1 display qos sp.....	4-1
4.1.2 qos sp.....	4-2
4.2 加权轮询队列配置命令.....	4-2
4.2.1 display qos wrr interface.....	4-2
4.2.2 qos wrr.....	4-3
4.2.3 qos wrr byte-count.....	4-4
4.2.4 qos wrr group sp.....	4-5
4.2.5 qos wrr weight.....	4-5
4.3 加权公平队列配置命令.....	4-6
4.3.1 display qos wfq interface.....	4-6
4.3.2 qos bandwidth queue.....	4-7
4.3.3 qos wfq.....	4-8
4.3.4 qos wfq byte-count.....	4-8
4.3.5 qos wfq group sp.....	4-9
4.3.6 qos wfq weight.....	4-10
5 拥塞避免配置命令.....	5-1
5.1 WRED配置命令.....	5-1
5.1.1 display qos wred interface.....	5-1
5.1.2 display qos wred table.....	5-1
5.1.3 qos wred apply.....	5-3
5.1.4 qos wred queue table.....	5-3
5.1.5 queue.....	5-4
6 数据缓冲区配置命令.....	6-1
6.1 自动配置数据缓冲区的命令.....	6-1

6.1.1 burst-mode enable .....	6-1
6.2 手工配置数据缓冲区的命令 .....	6-1
6.2.1 buffer apply .....	6-2
6.2.2 buffer egress queue guaranteed .....	6-2
6.2.3 buffer egress shared .....	6-3
6.2.4 buffer egress total-shared .....	6-4

# 1 QoS策略配置命令

---



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
<b>acl</b> [ ipv6 ] { <i>acl-number</i>   <b>name</b> <i>acl-name</i> }	定义匹配 ACL 的规则 <i>acl-number</i> 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 <i>acl-name</i> 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
<b>any</b>	定义匹配所有数据包的规则
<b>dscp</b> <i>dscp-list</i>	定义匹配DSCP的规则， <i>dscp-list</i> 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 <a href="#">表 1-4</a> 中的关键字
<b>destination-mac</b> <i>mac-address</i>	定义匹配目的 MAC 地址的规则
<b>customer-dot1p</b> <i>8021p-list</i>	定义匹配用户网络 802.1p 优先级的规则， <i>8021p-list</i> 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
<b>service-dot1p</b> <i>8021p-list</i>	定义匹配运营商网络 802.1p 优先级的规则， <i>8021p-list</i> 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
<b>ip-precedence</b> <i>ip-precedence-list</i>	定义匹配 IP 优先级的规则， <i>ip-precedence-list</i> 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
<b>protocol</b> <i>protocol-name</i>	定义匹配协议的规则， <i>protocol-name</i> 取值为 ip 或 ipv6
<b>source-mac</b> <i>mac-address</i>	定义匹配源 MAC 地址的规则

取值	描述
<b>customer-vlan-id</b> { <i>vlan-id-list</i>   <i>vlan-id1 to vlan-id2</i> }	定义匹配用户网络 VLAN ID 的规则， <i>vlan-id-list</i> 为 VLAN ID 的列表，最多可以输入 8 个 VLAN ID， <i>vlan-id1 to vlan-id2</i> 表示一个 VLAN ID 的范围， <i>vlan-id1</i> 的值必须小于 <i>vlan-id2</i> 的值，VLAN ID 取值范围为 1~4094
<b>service-vlan-id</b> { <i>vlan-id-list</i>   <i>vlan-id1 to vlan-id2</i> }	定义匹配运营商网络 VLAN ID 的规则， <i>vlan-id-list</i> 为 VLAN ID 的列表，最多可以输入 8 个 VLAN ID， <i>vlan-id1 to vlan-id2</i> 表示一个 VLAN ID 的范围， <i>vlan-id1</i> 的值必须小于 <i>vlan-id2</i> 的值，VLAN ID 取值范围为 1~4094
<b>system-index</b> <i>index-value-list</i>	定义规则来匹配预定义的上送控制平面报文类型， <i>index-value-list</i> 为系统预定义匹配字段索引号 ( <i>system-index</i> ) 的列表，最多可以输入 8 个 <i>system-index</i> 值， <i>system-index</i> 值的取值范围为 1~128



#### 说明

如果指定类的逻辑关系为 **and**，使用 **if-match** 命令定义匹配规则时，有如下注意事项：

- 匹配规则含有 **acl** 或 **acl ipv6** 时，如果在类中配置了多条这样的匹配规则，在应用策略时，匹配 **acl** 或 **acl ipv6** 的规则之间的逻辑关系实际为 **or**。
- 匹配规则含有 **customer-vlan-id** 或 **service-vlan-id** 时，如果在类中配置了多条这样的匹配规则，在应用策略时，匹配 **customer-vlan-id** 或 **service-vlan-id** 的规则之间的逻辑关系实际为 **or**。



#### 说明

当流分类中各规则之间的逻辑关系为 **and** 时，对于以下匹配条件，用户虽然可以通过重复执行 **if-match** 命令来配置多条匹配不同取值的规则，或在一条规则中使用 *list* 形式输入多个匹配值，但在应用使用该类的 QoS 策略时，对应该类的流行为将会无法正常执行：

- **customer-dot1p** *8021p-list*
- **destination-mac** *mac-address* (不支持 *list* 形式)
- **dscp** *dscp-list*
- **ip-precedence** *ip-precedence-list*
- **service-dot1p** *8021p-list*
- **source-mac** *mac-address* (不支持 *list* 形式)
- **system-index** *index-value-list*

如果用户需要创建匹配以上某一字段多个取值的规则，需要在创建流分类时指定各规则之间的逻辑关系为 **or**，然后再通过多次执行 **if-match** 命令的方式来配置匹配多个值的规则。

#### 【描述】

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

在定义各个规则的时候，注意事项如下：

- (1) 定义匹配 **ACL** 的规则
  - 如果类中引用的 **ACL** 不存在，则不能在硬件中下发。
  - 对同一个类，允许通过 **ACL** 名称和序号的方式分别引用一次同一个 **ACL**。
- (2) 定义匹配目的 **MAC** 地址和源 **MAC** 地址规则

- 一个类下可配置多条这样的命令，各个配置之间互相不覆盖。
- (3) 定义匹配 DSCP 的规则
- 一个类下可配置多条这样的命令，各个配置之间互相不覆盖。每条命令在配置后，*dscp* 值将自动按照从小到大的顺序排序。
  - 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) 定义匹配用户网络或运营商网络的 802.1p 优先级的规则
- 一个类下可配置多条这样的命令，各个配置之间互相不覆盖。每条命令在配置后，*8021p* 值将自动按照从小到大的顺序排序。
  - 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
- 一个类下可配置多条这样的命令，各个配置之间互相不覆盖。每条命令在配置后，IP 优先级的值将自动按照从小到大的顺序排序。
  - 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) 定义匹配用户网络和运营商网络 VLAN ID 的规则
- 一个类下可配置多条这样的命令，各个配置之间互相不覆盖。每条命令在配置后，*vlan-id* 值将自动按照从小到大的顺序排序。
  - 一条命令可以配置多个 VLAN ID 值，如果指定了多个相同的 VLAN ID 值，系统默认为一个；多个不同的 VLAN ID 值是或的关系，即只要有一个值匹配，就算匹配这条规则。
  - 删除某条匹配 VLAN ID 的规则时，指定的所有 VLAN ID 值必须与该规则中定义的完全相同才会删除，顺序可不一样。
- (7) 定义匹配预定义的上送控制平面报文类型的规则
- 一个类下可配置多条这样的命令，各个配置之间互相不覆盖。
  - 一条命令可以配置多个 *system-index* 值，如果指定了多个相同的 *system-index* 值，系统默认为一个；多个不同的 *system-index* 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 *system-index* 的规则时，指定的所有 *system-index* 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。
  - 系统预定义的报文类型信息可以通过 **display qos policy control-plane pre-defined** 命令查看。

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：匹配用户网络 802.1p 优先级为 3。

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

# 定义类 **class1** 的匹配规则为：匹配运营商网络 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：匹配用户网络 VLAN ID 值为 1 或 6 或 9 的报文。

<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match customer-vlan-id 1 6 9
# 定义类 class1 的匹配规则为：匹配运营商网络 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
# 定义类匹配 qos-local-id 3。

<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match qos-local-id 3
# 在流分类 class1 中配置匹配系统预定义的字段索引号为 1 的报文类型。

```

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match system-index 1
```

### 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
undo accounting
```

#### 【视图】

流行为视图

#### 【缺省级别】

2: 系统级

#### 【参数】

无

#### 【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。

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

## 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 且必须为 64 的整数倍。

**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  $62.5 \times \text{committed-information-rate}$ ，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，缺省值为 4000，单位为 Byte。取值范围为 0~16000000。

**pir peak information rate**: 峰值速率，单位为 kbps。取值范围为 64~10000000 且必须为 64 的整数倍。

**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。

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
    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	行为的名称及其内容，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 <a href="#">1.2 定义流行为的命令</a>
Accounting enable	流量统计相关信息
Committed Access Rate	流量限速的相关信息
Green Action	对绿色报文的处理
Red Action	对红色报文的处理
Yellow Action	对黄色报文的处理
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 ] ] }  
[ fail-action { discard | forward } ] }
```

```
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**: 重定向到指定的接口。

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

**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**。

**fail-action { discard | forward }**: 当下一跳的地址不存在时, 对报文采取的处理动作。**discard** 表示丢弃此报文。**forward** 表示转发此报文。

#### 【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、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 | customer-dot1p-trust }
```

```
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。

**customer-dot1p-trust**: QoS 策略应用到端口后, 将内层 VLAN Tag 的 802.1p 优先级复制为外层 VLAN Tag 的 802.1p 优先级。如果报文只携带一层 Tag, 则配置不生效。

### 【描述】

**remark dot1p** 命令用来配置标记报文的 802.1p 优先级或内外层标签优先级复制功能。**undo remark dot1p** 命令用来取消配置。

需要注意的是, 命令 **remark dot1p 8021p** 和 **remark dot1p customer-dot1p-trust** 是覆盖关系。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
```

# 配置内外层标签优先级复制功能。

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

## 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** [ **green** | **red** | **yellow** ] **dscp** *dscp-value*

## undo remark [ green | red | yellow ] dscp

### 【视图】

流行为视图

### 【缺省级别】

2: 系统级

### 【参数】

**green**: 对绿色报文进行重标记。

**red**: 对红色报文进行重标记。

**yellow**: 对黄色报文进行重标记。

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

表1-4 DSCP 关键字与值的对应表

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

### 【描述】

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

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

### 【举例】

# 配置标记报文的 DSCP 值为 6。



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

### 1.2.9 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**，“三层技术-IP 路由命令参考/路由策略”中的命令 **route-policy** 和 **apply qos-local-id**。

#### 【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 control-plane

#### 【命令】

**control-plane slot slot-number**

#### 【视图】

系统视图

#### 【缺省级别】

2：系统级

#### 【参数】

**slot slot-number**：在 IRF 中，使用 **slot** 参数进入指定成员设备的控制平面视图。**slot-number** 的取值范围取决于当前 IRF 中的成员数量和编号情况。

#### 【描述】

**control-plane** 命令用来进入控制平面视图。

#### 【举例】

# 进入 2 号成员设备的控制平面视图。

```
<Sysname> system-view
[Sysname] control-plane 2
[Sysname-cp-slot2]
```

### 1.3.3 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 <b>traffic classifier</b> 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 <b>traffic behavior</b> 命令

### 1.3.4 display qos policy control-plane

#### 【命令】

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

## 【视图】

任意视图

## 【缺省级别】

1: 监控级

## 【参数】

**slot slot-number:** 显示指定成员设备的控制平面上应用 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。

**inbound:** 显示对进入控制平面的报文应用的 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 control-plane** 命令用来显示控制平面应用 QoS 策略的信息。

## 【举例】

# 显示 3 号成员设备的控制平面入方向的 QoS 策略信息。

```
<Sysname> display qos policy control-plane slot 3 inbound
Control-plane slot 3
  Direction: Inbound
  Policy: 1
    Classifier: 2
      Operator: AND
      Rule(s) : If-match system-index 10
      Behavior: 2
        Committed Access Rate:
          CIR 128 (kbps), CBS 8000 (byte), EBS 0 (byte)
          Red Action: discard
          Green : 12928(Bytes)
          Red   : 43904(Bytes)
        Filter Enable: deny
```

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

字段	描述
Control-plane	控制平面
Direction	对进控制平面（Inbound）/出控制平面（Outbound）的报文应用 QoS 策略，目前仅支持入方向
Policy	策略名称及其内容
Classifier	类的名称及其内容，内容可以有多种类型
Operator	分类规则之间的逻辑关系
Rule(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
Committed Access Rate	流量限速的相关信息

字段	描述
CIR	承诺信息速率，单位为 kbps
CBS	承诺突发尺寸，也就是容纳突发流量的令牌桶深度，单位为 byte
EBS	超出突发尺寸，在双令牌桶算法中超出突发流量超过承诺突发流量的部分，单位为 byte
Red Action	对红色报文的动作
Green	绿色报文的流量统计
Red	红色报文的流量统计
Filter Enable	包过滤的相关信息（deny 表示丢弃数据包；permit 表示允许数据包通过）
none	表示没有配置其他流行为

### 1.3.5 display qos policy control-plane pre-defined

#### 【命令】

```
display qos policy control-plane pre-defined [ 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:** 显示指定成员设备的系统预定义的控制平面策略信息。*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 control-plane pre-defined** 命令用来显示系统预定义的控制平面应用 QoS 策略的信息。

需要注意的是：如果不指定成员设备，则显示所有成员设备的系统预定义的控制平面应用 QoS 策略的信息。

#### 【举例】

# 显示 2 号成员设备上系统预定义的控制平面 QoS 策略的信息。

```
<Sysname> display qos policy control-plane pre-defined slot 2
=====
Pre-defined Control-plane Policy Slot 2
-----
Index | PacketType          | Priority | BandWidth(Kbps)
-----
```

1	ISIS	4	256
29	ARP	1	64
30	ARP_REPLY	1	64
35	DOT1X	1	64
36	STP	6	128
37	LACP	5	64
38	GVRP	3	256
41	ICMP	1	512
53	LLDP	3	64
54	DLDP	3	64
106	IPV6_CPUDST_CAR	3	128

表1-7 display qos policy control-plane pre-defined 命令显示信息描述表

字段	描述
Pre-defined Control-plane Policy	预定义控制平面策略内容
Index	系统预定义匹配字段索引号
PacketType	匹配字段内容
Priority	优先级
BandWidth	带宽

### 1.3.6 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:** 显示设备所有接口入方向应用的 QoS 策略信息。

**outbound:** 显示设备所有接口出方向应用的 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 (Packets)
Committed Access Rate:
CIR 128 (kbps), CBS 8000 (Bytes), EBS 0 (Bytes)
Red Action: discard
Green : 12928(Packets)
Red : 43904(Packets)
```

```
Direction: Outbound
```

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

表1-8 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： <ul style="list-style-type: none"> <li>• 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全局正常应用</li> <li>• 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全局正常应用</li> </ul> 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



### 1.3.7 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*: 指定的接口类型和接口编号。

**inbound**: 显示对接口接收到的报文应用的 QoS 策略信息。

**outbound**: 显示对接口发送的报文应用的 QoS 策略信息。

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

**begin**: 从包含指定正则表达式的行开始显示。

**exclude**: 只显示不包含指定正则表达式的行。

**include**: 只显示包含指定正则表达式的行。

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

#### 【描述】

**display qos policy interface** 命令用来显示指定接口或所有接口上 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1-9 display qos policy interface 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号结合在一起组成。
Direction	Policy 应用在接口的方向
Policy	应用到接口上的策略的名字
Classifier	策略里分类规则以及对应的配置信息
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	策略里行为的名称及配置信息，参见 behavior 的相关命令

### 1.3.8 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。

#### 【举例】

# 显示 IRF 中 3 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 3
  Policy test
    Vlan 200: inbound
    Vlan 300: outbound

```

表1-10 display qos vlan-policy 命令显示信息描述表

字段	描述
Policy	QoS 策略名称
Vlan	应用 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(Packets)
        Red   : 43904(Packets)

Direction: Outbound

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

```

表1-11 display qos vlan-policy 命令显示信息描述表

字段	描述
Vlan	应用 QoS 策略的 VLAN ID
Direction	对 VLAN 接收到 (Inbound) /发送 (Outbound) 的报文应用 QoS 策略

字段	描述
Classifier	<p>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；</p> <p>在 IRF 中：</p> <ul style="list-style-type: none"> <li>如果在没有使用 <b>slot</b> 参数的情况下显示“(Failed)”，表示该关联组没有在 IRF 上正常应用</li> <li>如果在使用了 <b>slot</b> 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</li> </ul> <p>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</p>
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

### 1.3.9 qos apply policy (interface view, port group view, control plane view)

#### 【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/端口组视图/控制平面视图

#### 【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 的入方向上。

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

# 对进入 IRF 中 3 号成员设备控制平面的报文应用策略 aaa。

```
<Sysname> system-view
[Sysname] control-plane slot 3
[Sysname-cp-slot3] qos apply policy aaa inbound
```

### 1.3.10 qos apply policy (user-profile view)

#### 【命令】

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

## 【视图】

user-profile 视图

## 【缺省级别】

2: 系统级

## 【参数】

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

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

**policy-name:** 策略名，为 1~31 个字符的字符串。

## 【描述】

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

需要注意的是：

- 如果 User Profile 处于激活状态，既不能修改策略的内容（包括流分类引用的 ACL 规则），也不能删除已经应用到此 User Profile 的策略。
- 关联的策略只有在 User Profile 处于激活状态、且用户成功上线后才能生效。
- user-profile 视图下应用的策略中的流行为只支持 **remark**、**car**、**filter** 三种动作。
- user-profile 视图下应用的策略不能为空策略。

## 【举例】

# 对设备接收的上线用户 user 的流量应用策略 test（该策略已经建立）。

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

### 1.3.11 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。

## 【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
```

### 1.3.12 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]
```

### 1.3.13 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
```

### 1.3.14 reset qos policy control-plane

#### 【命令】

```
reset qos policy control-plane slot slot-number [ inbound ]
```

#### 【视图】

用户视图

#### 【缺省级别】

1: 监控级

#### 【参数】

**slot *slot-number***: 清除指定成员设备的控制平面应用 QoS 策略的统计信息。*slot-number* 的取值范围取决于当前 IRF 中的成员数量和编号情况。

**inbound**: 清除进入控制平面的方向的基于控制平面应用 QoS 策略的统计信息。

#### 【描述】

**reset qos policy control-plane** 命令用来清除控制平面应用 QoS 策略的统计信息。

#### 【举例】

# 清除应用到编号为 3 的成员设备控制平面上入方向的 QoS 策略统计信息。

```
<Sysname> reset qos policy control-plane slot 3 inbound
```

### 1.3.15 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。

如果不指定方向，则同时清除全局在入方向和出方向应用的 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
```

### 1.3.16 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。

如果不指定方向，则同时清除在 VLAN 入方向和出方向应用的 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 优先级映射配置命令



说明

优先级映射功能中的“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”。

### 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/端口组视图

#### 【缺省级别】

2: 系统级

#### 【参数】

**priority-value**: 端口优先级值，取值范围为 0~7。

#### 【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 GigabitEthernet 1/0/1 的优先级为 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

字段	描述
Port priority	端口优先级
Port priority trust type	优先级信任模式： <ul style="list-style-type: none"> <li>• dscp 表示信任报文的 DSCP 优先级</li> <li>• dot1p 表示信任报文的 802.1p 优先级</li> <li>• untrust 表示不信任报文携带的优先级</li> </ul>

## 2.3.2 qos trust

### 【命令】

```
qos trust { dot1p | dscp }
undo qos trust
```

### 【视图】

接口视图/端口组视图

### 【缺省级别】

2: 系统级

### 【参数】

**dot1p**: 信任报文自带的 802.1p 优先级，以此优先级进行优先级映射。

**dscp**: 信任 IP 报文自带的 DSCP，以此优先级进行优先级映射。

### 【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，设备不信任报文携带的优先级。

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

### 【举例】

# 在端口 GigabitEthernet 1/0/1 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/端口限速命令



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** 命令用来显示某个端口或所有端口的 GTS 配置情况。

如不指定端口，本命令将显示所有端口的 GTS 配置情况和运行统计信息。

#### 【举例】

# 显示所有端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), CBS 40960 (byte)
```

表3-1 display qos gts 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
Rule(s)	匹配规则。
CIR	承诺信息速率，单位为 kbps

字段	描述
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

### 3.1.2 qos gts

#### 【命令】

```
qos gts queue queue-number cir committed-information-rate [cbs committed-burst-size ]
undo qos gts queue queue-number
```

#### 【视图】

接口视图/端口组视图

#### 【缺省级别】

2: 系统级

#### 【参数】

**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。

**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，*committed-burst-size* 缺省取值为  $62.5\text{ms} * \text{committed-information-rate}$ ，且必须为 4096 的整数倍，如果乘积不是 4096 的整数倍，就取比乘积大的最近的 4096 的整数倍，但最大不会超过 16777216。
- 如果指定 **cbs** 参数，*committed-burst-size* 的取值范围为 4096~16777216，且必须为 4096 的整数倍。

#### 【描述】

**qos gts** 命令用来为某个队列的流设置整形参数，并开始整形。**undo qos gts** 命令用来取消对某一队列流的整形设置。

缺省情况下，端口上没有配置整形参数。

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

#### 【举例】

# 配置端口 GigabitEthernet 1/0/1 上队列 2 发送报文的速率为 640 kbps。

```
<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端口的端口限速配置情况。

如不指定端口，本命令将显示所有端口的端口限速配置情况。

## 【举例】

# 显示所有端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	端口名，由端口类型和端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 outbound cir committed-information-rate [ cbs committed-burst-size ]**

**undo qos lr outbound**

### 【视图】

接口视图/端口组视图

### 【缺省级别】

2: 系统级

### 【参数】

**outbound:** 对端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  $62.5\text{ms} * \text{committed-information-rate}$ ，且必须为 4000 的整数倍，如果乘积不是 4000 的整数倍，就取比乘积大的最近的 4000 的整数倍，但是最大值不能超过 16000000。
- 如果指定 **cbs** 参数，取值范围 4000~16000000 且必须是 4000 的倍数。

#### 【描述】

**qos lr** 命令用来限制端口的发送数据的速率。**undo qos lr** 命令用来取消限制。

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

#### 【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 拥塞管理配置命令



## 说明

拥塞管理功能中的“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”。

## 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】

# 显示端口 GigabitEthernet 1/0/1 的 SP 队列配置信息。

```
<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

字段	描述
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/端口组视图

### 【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 WRR 调度算法。

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

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

### 【举例】

# 在端口 GigabitEthernet 1/0/1 上配置使用 SP 调度算法。

```
<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** 命令用来显示接口的 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 GigabitEthernet 1/0/1 的 WRR 队列配置信息。

```
<Sysname> display qos wrr interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
Output queue: Weighted round robin queue
Queue ID      Group      Weight
-----
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
Weight	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/端口组视图

#### 【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。

#### 【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 WRR 队列进行调度。

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

#### 【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/端口组视图

#### 【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、9、13、15。

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。

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

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/端口组视图

### 【缺省级别】

2: 系统级

### 【参数】

*queue-id*: 队列序号，取值范围为 0~7。

*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。

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

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
```

## 4.2.5 qos wrr weight

### 【命令】

```
qos wrr queue-id group 1 weight schedule-value
undo qos wrr queue-id group 1 weight
```

### 【视图】

接口视图/端口组视图

### 【缺省级别】

2: 系统级

### 【参数】

*queue-id*: 队列序号，取值范围为 0~7。

**group 1**: 表示该队列属于 WRR 调度组。

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

#### 【描述】

**qos wrr weight** 命令用来配置 WRR 队列的调度权重（在使用报文个数为调度单位时）。**undo qos wrr weight** 命令用来将 WRR 队列参数恢复为缺省情况（在使用报文个数为调度单位时）。

缺省情况下，在使用报文个数为调度单位时，0~7 队列的调度权重分别为 1、2、3、4、5、9、13、15。

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 队列调度是以报文个数作为调度单位，以保证调度权重的配置能够正常生效。

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

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

#### 【举例】

# 在 GigabitEthernet1/0/1 上应用使用报文个数为调度单位的 WRR 队列，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 weight
[Sysname-GigabitEthernet1/0/1] qos wrr 0 group 1 weight 10
```

## 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           64
1             1          1           64
2             1          1           64
3             1          1           64
4             1          1           64
5             1          1           64
6             1          1           64
7             1          1           64

```

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，如果开启 WFQ 队列时选择的调度权重为报文个数，这里将显示 Weight，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

### 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/端口组视图

#### 【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 64~1000000。
- 万兆端口的取值范围为 64~10000000。

#### 【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，队列的最小保证带宽为 64kbps。

需要注意的是：



- 在接口视图下执行该命令，则该配置只在当前接口生效；在端口组视图下执行该命令，则该配置将在端口组中的所有端口生效。
- 在端口或端口组上开启 WFQ（Weighted Fair Queuing，加权公平队列）调度算法的情况下，才需要配置最小带宽保证。

#### 【举例】

# 在 GigabitEthernet 1/0/1 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/端口组视图

#### 【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。

#### 【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 WRR 调度算法。

需要注意的是：

- 在接口视图下执行该命令，则该配置只在当前接口生效；在端口组视图下执行该命令，则该配置将在端口组中的所有端口生效。
- 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，并使用报文个数作为调度权重。

```
<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/端口组视图

#### 【缺省级别】

2: 系统级

#### 【参数】

**queue-id**: 队列序号, 取值范围为 0~7。

**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。

#### 【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。

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

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/端口组视图

#### 【缺省级别】

2: 系统级

#### 【参数】

**queue-id**: 队列序号, 取值范围为 0~7。

**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, 不再采用加权公平调度算法。

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

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
```

### 4.3.6 qos wfq weight

#### 【命令】

```
qos wfq queue-id group 1 weight schedule-value
undo qos wfq queue-id group 1 weight
```

#### 【视图】

接口视图/端口组视图

#### 【缺省级别】

2: 系统级

#### 【参数】

**queue-id**: 队列序号，取值范围为 0~7。

**group 1**: 表示该队列属于 WFQ 调度组。

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

#### 【描述】

**qos wfq weight** 命令用来配置 WFQ 队列的调度权重（在使用报文个数为调度单位时）。**undo qos wfq weight** 命令用来将 WFQ 队列参数恢复为缺省情况（在使用报文个数为调度单位时）。

缺省情况下，在使用报文个数为调度单位时，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 WRR 队列调度权重前，请确认当前端口的 WRR 队列调度是以报文个数作为调度单位，以保证调度权重的配置能够正常生效。

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

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，使用报文个数为调度单位，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 weight
[Sysname-GigabitEthernet1/0/1] qos wfq 0 group 1 weight 10
```

# 5 拥塞避免配置命令



说明

拥塞避免功能中的“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”。

## 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
-----
0    10    NA    10    10    NA    10
1    10    NA    10    10    NA    10
2    10    NA    10    10    NA    10
3    10    NA    10    10    NA    10
4    10    NA    10    10    NA    10
5    10    NA    10    10    NA    10
6    10    NA    10    10    NA    10
7    10    NA    10    10    NA    10
```

表5-1 display qos wred table 命令显示信息描述表

字段	描述
Table name	WRED 表的名称
Table type	WRED 表的类型
QID	队列编号
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

### 5.1.3 qos wred apply

#### 【命令】

```
qos wred apply table-name  
undo qos wred apply
```

#### 【视图】

接口视图/端口组视图

#### 【缺省级别】

2: 系统级

#### 【参数】

*table-name*: WRED 表的名称, 为 1~32 个字符的字符串。

#### 【描述】

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

缺省情况下, 端口或端口组上没有应用 WRED 表。

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

#### 【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
```

## 5.1.5 queue

### 【命令】

```
queue queue-value [ drop-level drop-level ] low-limit low-limit [ discard-probability discard-prob ]  
undo queue { queue-value | all }
```

### 【视图】

WRED 表视图

### 【缺省级别】

2: 系统级

### 【参数】

**queue-value**: 队列编号，取值范围为 0~7。

**drop-level drop-level**: 丢弃级别，取值范围为 0~1。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**: 队列占用率下限，当队列中报文占用队列缓存的比例超过下限时，开始丢弃报文。占用率下限的取值范围为 1~100，缺省值为 10。

**discard-probability discard-prob**: 丢弃概率的倒数，**discard-prob** 的取值范围为 0~128，缺省值为 10，可针对每个丢弃级别进行设置。

- 当 **discard-prob** 参数设置为 0 时，丢弃概率为 100%；
- 当 **discard-prob** 参数设置为 1~8 时，丢弃概率为 1/8；
- 当 **discard-prob** 参数设置为 9~16 时，丢弃概率为 1/16；
- 当 **discard-prob** 参数设置为 17~32 时，丢弃概率为 1/32；
- 当 **discard-prob** 参数设置为 33~64 时，丢弃概率为 1/64；
- 当 **discard-prob** 参数设置为 65~128 时，丢弃概率为 1/128

### 【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 表中所有丢弃级别的报文的队列占用率下限为 10，计算丢弃概率的参数为 10。相关配置可参考命令 **qos wred queue table**。

### 【举例】

# 修改 WRED 表 queue-table1 的队列 1 的丢弃参数，将丢弃级别为 1 的报文的队列占用率下限配置为 10，计算丢弃概率的参数为 30。

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

```
[Sysname] qos wred queue table queue-table1
```

```
[Sysname-wred-table-queue-table1] queue 1 drop-level 1 low-limit 10 discard-probability 30
```

# 6 数据缓冲区配置命令

## 6.1 自动配置数据缓冲区的命令

### 6.1.1 burst-mode enable

#### 【命令】

**burst-mode enable**  
**undo burst-mode enable**

#### 【视图】

系统视图

#### 【缺省级别】

2: 系统级

#### 【参数】

无

#### 【描述】

**burst-mode enable** 命令用来开启 Burst 功能。**undo burst-mode enable** 命令用来关闭 Burst 功能。

缺省情况下，Burst 功能处于关闭状态。

用户可以通过开启 Burst 功能，使交换机自动分配 **cell** 资源和 **packet** 资源的共享区域比例、队列的最小保证资源比、队列和端口的最大共享资源占用比，来获得更好的报文缓存功能和流量转发性能。



说明

**burst-mode enable** 命令与手工配置数据缓冲区的所有命令均不能同时配置。

#### 【举例】

# 开启 Burst 功能。

```
<Sysname> system-view  
[Sysname] burst-mode enable
```

## 6.2 手工配置数据缓冲区的命令



说明

- 数据缓冲区的配置比较复杂，而且对设备的转发功能有重要的影响，建议用户不要轻易修改数据缓冲区的参数。在需要较大的缓存空间时，建议使用 Burst 功能来自动分配缓冲区。
- 本节中介绍的所有命令与 **burst-mode enable** 命令均不能同时配置。



## 6.2.1 buffer apply

### 【命令】

**buffer apply**  
**undo buffer apply**

### 【视图】

系统视图

### 【缺省级别】

2: 系统级

### 【参数】

无

### 【描述】

**buffer apply** 命令用来应用用户对数据缓冲区所做的配置。**undo buffer apply** 命令用来恢复数据缓冲区的配置为缺省情况。

缺省情况下，本系列交换机的数据缓冲区各项配置参数如 [表 6-1](#) 所示。

表6-1 缺省缓冲区参数

资源类型	共享区域比例	队列的最小保证资源比	端口的最大共享资源占用比
cell 资源	50%	12%	50%
packet 资源	-	队列 2 为 51%，其余队列均为 7%	-

### 【举例】

# 应用数据缓冲区的配置。

```
<Sysname> system-view  
[Sysname] buffer apply
```

## 6.2.2 buffer egress queue guaranteed

### 【命令】

**buffer egress [ slot slot-number ] { cell | packet } queue queue-id guaranteed ratio ratio**  
**undo buffer egress [ slot slot-number ] { cell | packet } queue queue-id guaranteed**

### 【视图】

系统视图

### 【缺省级别】

2: 系统级

### 【参数】

**slot slot-number**: 成员设备编号。在 IRF 中配置该命令时，如果指定了 **slot-number**，表示配置指定编号的成员设备的缓冲资源，如果没有指定 **slot-number**，则表示配置 IRF 中所有成员设备的缓冲资源。

**cell**: 配置队列在 **cell** 资源中的最小保证资源比。

**packet**: 配置队列在 **packet** 资源中的最小保证资源比。

**queue-id**: 需要配置的队列编号，取值范围为 0~7。

**ratio**: 队列的最小保证资源比, 以百分数形式表示, 取值范围为 0~100。

#### 【描述】

**buffer egress queue guaranteed** 命令用来配置队列在 **cell** 资源或 **packet** 资源中的最小保证资源比。**undo buffer egress queue guaranteed** 命令用来恢复队列最小保证资源比的缺省情况。

缺省情况下, 在 **cell** 缓冲区中, 所有队列的最小保证资源比均为 12%; 在 **packet** 缓冲区中, 队列 2 的最小保证缓存比为 51%, 其余队列均为 7%。

---

#### 说明

- 由于端口的独享资源是由 8 个队列共同使用, 因此当用户修改了某个队列的最小保证资源比之后, 其它队列的最小保证资源比将随之自动变化, 自动变化的原则为: 除用户手工配置的最小保证资源比之外, 剩余比例将平均分配给未进行手工配置的队列。例如, 如果配置一个队列的最小保证资源比为 30%, 则剩余 7 个队列的最小保证资源比将自动变化为 10%。
- 队列的最小保证资源比对全局生效, 即配置后每个端口上的该队列均能以相同的比例占用当前端口的独享资源。

---

#### 【举例】

# 配置队列 0 在 **cell** 资源中的最小保证资源比为 20%。

```
<Sysname> system-view  
[Sysname] buffer egress cell queue 0 guaranteed ratio 20
```

# 在 IRF 中, 配置指定成员设备(编号为 2)的队列 0 在该设备 **cell** 资源中的最小保证资源比为 15%。

```
<Sysname> system-view  
[Sysname] buffer egress slot 2 cell queue 0 guaranteed ratio 15
```

### 6.2.3 buffer egress shared

#### 【命令】

**buffer egress [ slot slot-number ] cell shared ratio ratio**

**undo buffer egress [ slot slot-number ] cell shared**

#### 【视图】

系统视图

#### 【缺省级别】

2: 系统级

#### 【参数】

**slot slot-number**: 成员设备编号。在 IRF 中配置该命令时, 如果指定了 **slot-number**, 表示配置指定编号的成员设备的缓冲资源, 如果没有指定 **slot-number**, 则表示配置 IRF 中所有成员设备的缓冲资源。

**cell**: 配置端口在 **cell** 缓冲区中的最大共享资源占用比。

**ratio**: 端口的最大共享资源占用比, 以百分数形式表示, 取值范围为 0~100。

#### 【描述】

**buffer egress shared** 命令用来配置端口在 **cell** 缓冲区中的最大共享资源占用比。**undo buffer egress shared** 命令用来恢复端口最大共享资源占用比的缺省情况。

缺省情况下, 所有端口在 **cell** 缓冲区中的最大共享资源占用比均为 50%。



说明

端口的最大共享资源占用比对所有端口生效，即配置后每个端口均能够以相同的最大共享资源占用比来动态使用共享区域资源。

#### 【举例】

# 配置当前设备上所有端口在 **cell** 缓冲区中的最大共享资源占用比为 30%。

```
<Sysname> system-view
[Sysname] buffer egress cell shared ratio 30
```

# 在 IRF 中，配置指定成员设备（编号为 2）的所有端口在该设备 **cell** 缓冲区中的最大共享资源占用比为 40%。

```
<Sysname> system-view
[Sysname] buffer egress slot 2 cell shared ratio 40
```

### 6.2.4 buffer egress total-shared

#### 【命令】

```
buffer egress [ slot slot-number ] cell total-shared ratio ratio
undo buffer egress [ slot slot-number ] cell total-shared
```

#### 【视图】

系统视图

#### 【缺省级别】

2: 系统级

#### 【参数】

**slot slot-number**: 成员设备编号。在 IRF 中配置该命令时，如果指定了 *slot-number*，表示配置指定编号的成员设备的缓冲资源，如果没有指定 *slot-number*，则表示配置 IRF 中所有成员设备的缓冲资源。

**cell**: 配置 **cell** 缓冲区中的共享区域所占比例。

**ratio**: 共享区域所占的比例，以百分数形式表示，取值范围为 0~100。

#### 【描述】

**buffer egress total-shared** 命令用来配置 **cell** 缓冲区中的共享区域所占的比例。**undo buffer egress total-shared** 命令用来恢复 **cell** 缓冲区中共享区域所占比例的缺省值。

缺省情况下，本系列交换机的 **cell** 缓冲区中共享区域所占比例为 50%。

#### 【举例】

# 配置当前设备 **cell** 缓冲区中的共享区域所占比例为 50%。

```
<Sysname> system-view
[Sysname] buffer egress cell total-shared ratio 50
```

# 在 IRF 中，配置指定成员设备（编号为 2）的 **cell** 缓冲区中共享区域所占比例为 65%。

```
<Sysname> system-view
[Sysname] buffer egress slot 2 cell total-shared ratio 65
```