H3C E528 & E552 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：6W100-20130425
产品版本：Release 1513

前 言

H3C E528 & E552 以太网交换机命令参考共分为十本手册，主要针对 E528 & E552 以太网交换机 Release 1513 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

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

无

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... } *	表示从多个选项中至少选取一个。
[x | y | ...] *	表示从多个选项中选取一个、多个或者不选。

格　式	意　义
&<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。

产品配套资料

H3C E528 & E552 以太网交换机的配套资料包括如下部分：

大类	资料名称	内容介绍
产品知识介绍	产品彩页	帮助您了解产品的主要规格参数及亮点
	RPS电源用户手册	帮助您了解产品支持的RPS电源的外观、功能、规格
	H3C低端系列以太网交换机RPS电源选购指南	帮助您了解各种RPS电源适用的交换机产品型号及RPS电源配套电缆的相关规格
	H3C低端系列以太网交换机可插拔模块手册	帮助您了解产品支持的可插拔模块类型、外观和规格
设备安装	安全兼容性手册	列出产品的兼容性声明，并对兼容性和安全的细节进行说明
	H3C 设备防雷安装指导手册	帮助您了解防雷接地设计和工程安装方法，以保证交换机具有良好的抗雷击性能
	快速安装指南	指导您对设备进行初始安装，通常针对最常用的情况，减少您的检索时间
	安装手册	帮助您详细了解设备硬件规格和安装方法，指导您对设备进行安装
	H3C可插拔SFP[SFP+][XFP]模块安装指南	帮助您掌握SFP/SFP+/XFP模块的正确安装方法，避免因操作不当而造成器件损坏
业务配置	配置指导	帮助您掌握设备软件功能的配置方法及配置步骤
	命令参考	详细介绍设备的命令，相当于命令字典，方便您查阅各个命令的功能
运行维护	故障处理手册	指导您快速定位并处理软件故障
	版本说明书	帮助您了解产品版本的相关信息（包括：版本配套说明、兼容性说明、特性变更说明、技术支持信息）及软件升级方法

资料获取方式

您可以通过H3C网站（www.h3c.com.cn）获取最新的产品资料：

H3C 网站与产品资料相关的主要栏目介绍如下：

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

技术支持

用户支持邮箱：service@h3c.com

技术支持热线电话：400-810-0504（手机、固话均可拨打）

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

感谢您的反馈，让我们做得更好！

目 录

1 ACL配置命令

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 IPv4 ACL 的编号。*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；

name *acl-name*：指定 IPv4 ACL 的名称。*acl-name* 表示 IPv4 ACL 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，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。

【描述】

acl 命令用来创建一个 IPv4 ACL，并进入相应的 ACL 视图。**undo acl** 命令用来删除 IPv4 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 IPv4 ACL 不存在，则创建该 ACL 并进入其视图，否则直接进入其视图。
- 用户只能在创建 ACL 时为其指定名称，ACL 一旦创建，便不允许对其名称进行修改或删除。
- 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 IPv4 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 IPv4 ACL 的名称，该 ACL 必须存在。*source-acl-name* 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。

dest-acl-number：指定目的 IPv4 ACL 的编号，该 ACL 必须不存在。若未指定本参数，系统将为目的 IPv4 ACL 自动分配一个与源 IPv4 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 IPv4 ACL 的名称，该 ACL 必须不存在。*dest-acl-name* 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，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 IPv4 ACL 指定名称。

【描述】

acl copy 命令用来复制生成一个新的同类型 IPv4 ACL。

需要注意的是：

- 目的 IPv4 ACL 的类型要与源 IPv4 ACL 的类型相同。
- 目的 IPv4 ACL 的名称只能在复制时指定，且目的 IPv4 ACL 一旦生成，便不允许对其名称进行修改或删除。
- 除了 ACL 的编号和名称不同外，新生成的 IPv4 ACL（即目的 IPv4 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 IPv4 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 1～32 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，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。
- 用户只能在创建 ACL 时为其指定名称，ACL 一旦创建，便不允许对其名称进行修改或删除。
- 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 1～32 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。

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 IP64 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 1～32 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，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 指定名称。

【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指定，且目的 IPv6 ACL 一旦生成，便不允许对其名称进行修改或删除。
- 除了 ACL 的编号和名称不同外，新生成的 IPv6 ACL（即目的 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 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 1～32 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。

【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]
```

1.1.6 acl name

【命令】

acl name *acl-name*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

acl-name：指定 IPv4 ACL 的名称，该 ACL 必须存在。本参数为 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。

【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]
```

1.1.7 description

【命令】

description *text*

undo description

【视图】

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

【缺省级别】

2：系统级

【参数】

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

【描述】

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

缺省情况下，ACL 没有任何描述信息。

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

【举例】

为基本 IPv4 ACL 2000 配置描述信息。

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

1.1.8 display acl

【命令】

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

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

acl-number：显示指定编号的 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 1～32 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。

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。

|：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“基本配置指导”中的“CLI 配置”。

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, 2 rules,
ACL's step is 5
 rule 0 permit
 rule 5 permit source 1.1.1.1 0 (5 times matched)

Basic ACL  2001, named -none-, 3 rules, match-order is auto,
ACL's step is 5
 rule 10 permit source 192.168.1.0 0.0.0.255
 rule 10 comment This rule is used in VLAN 2.
 rule 5 permit source 2.2.2.2 0
 rule 0 permit
```

表1-1 display acl 命令显示信息描述表

字段	描述
Basic ACL 2000	该ACL的类型和编号，ACL的类型包括： • Basic ACL：表示 IPv4 基本 ACL • Advanced ACL：表示 IPv4 高级 ACL • Ethernet frame ACL：表示二层 ACL
named flow	该ACL的名称为flow，-none-表示没有名称
2 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）
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，仅统计软件IPv4 ACL的匹配次数（匹配次数为0时不显示本字段）
rule 10 comment This rule is used in VLAN 2.	规则10的描述信息为rule 10 comment This rule is used in VLAN 2.

1.1.9 display acl ipv6

【命令】

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

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

acl6-number：显示指定编号的 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 1～32 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。

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。

|：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 配置”。

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,
 ACL's step is 5
 rule 0 permit
 rule 5 permit source 1::/64
 rule 10 permit source 1::1/128 (5 times matched)

 Basic IPv6 ACL  2001, named -none-, 3 rules, match-order is auto,
 ACL's step is 5
 rule 10 permit source 1::1/128
 rule 10 comment This rule is used on GE 1/0/1.
 rule 5 permit source 1::/64
 rule 0 permit
```

表1-2 display acl ipv6 命令显示信息描述表

字段	描述
Basic IPv6 ACL 2000	该ACL的类型和编号，ACL的类型包括： • Basic IPv6 ACL：表示 IPv6 基本 ACL • Advanced IPv6 ACL：表示 IPv6 高级 ACL
named flow	该ACL的名称为flow，-none-表示没有名称（简单ACL没有本字段）
3 rule	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）

字段	描述
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，仅统计软件IPv6 ACL的匹配次数（匹配次数为0时不显示本字段）
rule 10 comment This rule is used on GE 1/0/1.	规则10的描述信息为rule 10 comment This rule is used on GE 1/0/1.

1.1.10 display acl resource

【命令】

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

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

slot *slot-number*：显示 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，交换机形成 IRF 时，显示 IRF 中所有交换机 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 配置”。

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】

显示交换机 ACL 资源的使用情况。

```
<Sysname> display acl resource
-------------------------------------------------
 GE1/0/1..GE1/0/24
 GE1/0/49 GE1/0/50
-------------------------------------------------
  Type       Total   Reserved  Configured  Remaining
-------------------------------------------------
  ACL        1024    388       0           636
  Meter      64      0         0           64
-------------------------------------------------
 GE1/0/25..GE1/0/48
 GE1/0/51 GE1/0/52
-------------------------------------------------
  Type       Total   Reserved  Configured  Remaining
-------------------------------------------------
```

```
ACL          1024    388         0           636
Meter        64      0           0           64
```

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： • ACL 表示 ACL 规则资源 • Meter 表示流量监管资源
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	剩余的ACL规则数

1.1.11 display packet-filter

【命令】

display packet-filter { { **all** | **interface** *interface-type interface-number* } [**inbound**] | **interface vlan-interface** *vlan-interface-number* [**inbound**] [**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。

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 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 配置”。

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。

【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
```

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	入方向上报文过滤策略的应用情况
acl 2001, Successful	应用IPv4 ACL 2001成功

1.1.12 display time-range

【命令】

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

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

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

all：显示所有时间段的配置和状态信息。

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

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 trname 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： • 时间段的名称 • 时间段的状态，包括 Active（生效）和 Inactive（未生效）两种状态 • 时间段的时间范围

1.1.13 packet-filter

【命令】

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

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

【视图】

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 1～32 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。

inbound：对端口/接口收到的 IPv4 报文进行过滤。

【描述】

packet-filter 命令用来在端口/接口上应用 ACL 对 IPv4 报文进行过滤。**undo packet-filter** 命令用来恢复缺省情况。

缺省情况下，在端口/接口上不对 IPv4 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 IPv4 报文进行过滤。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEtherhet1/0/1] packet-filter 2001 inbound
```

1.1.14 packet-filter ipv6

【命令】

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

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

【视图】

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 1～32 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。

inbound：对接口收到的 IPv6 报文进行过滤。

【描述】

packet-filter ipv6 命令用来在端口/接口上应用 ACL 对 IPv6 报文进行过滤。**undo packet-filter ipv6** 命令用来恢复缺省情况。

缺省情况下，在端口/接口上不对 IPv6 报文进行过滤。

相关配置可参考命令 **display packet-filter ipv6**。

【举例】

应用 IPv6 ACL 2500 对端口 GigabitEthernet1/0/1 收到的 IPv6 报文进行过滤。

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

1.1.15 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 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：指定所有的 IPv4 ACL。

name *acl-name*：指定 IPv4 ACL 的名称。*acl-name* 表示 IPv4 ACL 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。

【描述】

reset acl counter 命令用来清除 IPv4 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 的基本 IPv4 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
```

1.1.16 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 1～32 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。

【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 的基本 IPv6 ACL 的统计信息。

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

清除名为 flwo 的 IPv6 ACL 的统计信息。

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

1.1.17 rule (Ethernet frame header ACL view)

【命令】

rule [*rule-id*] { **deny** | **permit** } [**cos** *vlan-pri* | **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* [**fragment** | **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。

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。

【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** 和 **step**。


说明

当二层 ACL 被 QoS 策略引用对报文进行流分类时，不支持配置 **lsap** 参数。

【举例】

为二层 ACL 4000 创建一条规则，拒绝 802.1p 优先级为 3 的报文。

```
<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] rule deny cos 3
```

1.1.18 rule (IPv4 basic ACL view)

【命令】

rule [*rule-id*] { **deny** | **permit** } [**fragment** | **source** { *sour-addr sour-wildcard* | **any** } | **time-range** *time-range-name*] *

undo rule *rule-id* [**fragment** | **source** | **time-range**] *

【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。

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，则表示该规则对非分片报文和分片报文均有效。

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。

【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** 和 **step**。

【举例】

为 IPv4 基本 ACL 2000 创建一条规则，拒绝源地址为 1.1.1.1/32 的报文。

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

```
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule deny source 1.1.1.1 0
```

1.1.19 rule (IPv4 advanced ACL view)

【命令】

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **destination** { *dest-addr dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | **dscp** *dscp* | **fragment** | **icmp-type** { *icmp-type icmp-code* | *icmp-message* } | **precedence** *precedence* | **reflective** | **source** { *sour-addr sour-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name* | **tos** *tos*] *

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

【视图】

IPv4 高级 ACL 视图

【缺省级别】

2：系统级

【参数】

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

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

protocol：表示 IPv4 承载的协议类型，可输入的形式如下：

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

*protocol*之后可配置如 表 1-6 所示的规则信息参数。

表1-6 规则信息参数

参数	类别	作用	说明
source { *sour-addr sour-wildcard* | **any** }	源地址信息	指定ACL规则的源地址信息	*sour-addr sour-wildcard*：源IP地址及其通配符掩码（为0表示主机地址） **any**：任意源IP地址
destination { *dest-addr dest-wildcard* | **any** }	目的地址信息	指定ACL规则的目的地址信息	*dest-addr dest-wildcard*：目的IP地址及其通配符掩码（为0表示主机地址） **any**：任意目的IP地址
precedence *precedence*	报文优先级	IP优先级	*precedence*：用数字表示时，取值范围为0～7；用名称表示时，为**routine**、**priority**、**immediate**、**flash**、**flash-override**、**critical**、**internet**或**network**，分别对应于数字0～7
tos *tos*	报文优先级	ToS优先级	*tos*：用数字表示时，取值范围为0～15；用名称表示时，可选取**max-reliability**（2）、**max-throughput**（4）、**min-delay**（8）、**min-monetary-cost**（1）或**normal**（0）

参数	类别	作用	说明
dscp *dscp*	报文优先级	DSCP优先级	*dscp*：用数字表示时，取值范围为0～63；用名称表示时，可选取**af11**（10）、**af12**（12）、**af13**（14）、**af21**（18）、**af22**（20）、**af23**（22）、**af31**（26）、**af32**（28）、**af33**（30）、**af41**（34）、**af42**（36）、**af43**（38）、**cs1**（8）、**cs2**（16）、**cs3**（24）、**cs4**（32）、**cs5**（40）、**cs6**（48）、**cs7**（56）、**default**（0）或**ef**（46）
reflective	自反标志	设置规则具有自反属性	目前不支持该参数
fragment	分片信息	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，则表示该规则对非分片报文和分片报文均有效
time-range *time-range-name*	时间段信息	指定规则生效的时间段	*time-range-name*：时间段的名称，为1～32个字符的字符串，不区分大小写，必须以英文字母a～z或A～Z开头

注意

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

当*protocol*为**tcp**（6）或**udp**（17）时，用户还可配置如 表 1-7 所示的规则信息参数。

表1-7 TCP/UDP 特有的规则信息参数

参数	类别	作用	说明
source-port *operator port1* [*port2*]	源端口	定义TCP/UDP报文的源端口信息	*operator*：操作符，取值可以为**lt**（小于）、**gt**（大于）、**eq**（等于）、**neq**（不等于）或者**range**（在范围内，包括边界值）。只有**range**操作符需要两个端口号做操作数，其它操作符只需要一个端口号做操作数
destination-port *operator port1* [*port2*]	目的端口	定义TCP/UDP报文的目的端口信息	*port1*/*port2*：TCP或UDP的端口号，用数字表示时，取值范围为0～65535；用名称表示时，TCP端口号可选取**chargen**（19）、**bgp**（179）、**cmd**（514）、**daytime**（13）、**discard**（9）、**domain**（53）、**echo**（7）、**exec**（512）、**finger**（79）、**ftp**（21）、**ftp-data**（20）、**gopher**（70）、**hostname**（101）、**irc**（194）、**klogin**（543）、**kshell**（544）、**login**（513）、**lpd**（515）、**nntp**（119）、**pop2**（109）、**pop3**（110）、**smtp**（25）、**sunrpc**（111）、**tacacs**（49）、**talk**（517）、**telnet**（23）、**time**（37）、**uucp**（540）、**whois**（43）或**www**（80）；UDP端口号可选取**biff**（512）、**bootpc**（68）、**bootps**（67）、**discard**（9）、**dns**（53）、**dnsix**（90）、**echo**（7）、**mobilip-ag**（434）、**mobilip-mn**（435）、**nameserver**（42）、**netbios-dgm**（138）、**netbios-ns**（137）、**netbios-ssn**（139）、**ntp**（123）、**rip**（520）、**snmp**（161）、**snmptrap**（162）、**sunrpc**（111）、**syslog**（514）、**tacacs-ds**（65）、**talk**（517）、**tftp**（69）、**time**（37）、**who**（513）或**xdmcp**（177）

参数	类别	作用	说明
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	TCP报文标识	定义对携带不同标志位（包括ACK、FIN、PSH、RST、SYN和URG六种）的TCP报文的处理规则	TCP协议特有的参数。表示匹配携带不同标志位的TCP报文，各*value*的取值可为0或1（0表示不携带此标志位，1表示携带此标志位） 如果在一条规则中设置了多个TCP标志位的匹配值，则这些匹配条件之间的关系为“与”
established	TCP连接建立标识	定义对TCP连接报文的处理规则	该参数用于定义TCP报文中ACK或RST标志位为1的报文

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

表1-8 ICMP 特有的规则信息参数

参数	类别	作用	说明
icmp-type { *icmp-type* *icmp-code* | *icmp-message* }	ICMP报文的消息类型和消息码信息	指定规则的ICMP报文的消息类型和消息码信息	*icmp-type*：ICMP消息类型，取值范围为0～255 *icmp-code*：ICMP的消息码，取值范围为0～255 *icmp-message*：ICMP消息的名称。可输入的ICMP消息名称，及其与消息类型和消息码的对应关系如表1-9所示

表1-9 ICMP 消息名称与消息类型和消息码的对应关系

名称	ICMP TYPE	ICMP CODE
echo	Type=8	Code=0
echo-reply	Type=0	Code=0
fragmentneed-DFset	Type=3	Code=4
host-redirect	Type=5	Code=1
host-tos-redirect	Type=5	Code=3
host-unreachable	Type=3	Code=1
information-reply	Type=16	Code=0
information-request	Type=15	Code=0
net-redirect	Type=5	Code=0
net-tos-redirect	Type=5	Code=2
net-unreachable	Type=3	Code=0
parameter-problem	Type=12	Code=0
port-unreachable	Type=3	Code=3
protocol-unreachable	Type=3	Code=2
reassembly-timeout	Type=11	Code=1
source-quench	Type=4	Code=0
source-route-failed	Type=3	Code=5
timestamp-reply	Type=14	Code=0
timestamp-request	Type=13	Code=0
ttl-exceeded	Type=11	Code=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** 和 **step**。

【举例】

为 IPv4 高级 ACL 3000 创建一条规则，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 TCP 连接。

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

1.1.20 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** } | **destination** { *dest dest-prefix* | *dest/dest-prefix* | **any** } | **destination-port** *operator port1* [*port2*] | **dscp** *dscp* | **flow-label** *flow-label-value* | **fragment** | **icmpv6-type** { *icmpv6-type icmpv6-code* | *icmpv6-message* } | **source** { *source source-prefix* | *source/source-prefix* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name*] *

undo rule *rule-id* [{ { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **established** } | **destination** | **destination-port** | **dscp** | **flow-label** | **fragment** | **icmpv6-type** | **source** | **source-port** | **time-range**] *

【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
source { *source source-prefix* | *source/source-prefix* | **any** }	源IPv6地址信息	指定IPv6 ACL规则的源IPv6地址信息	*source*：源IPv6地址 *source-prefix*：前缀长度，取值范围1～128 **any**：任意源IPv6地址
destination { *dest dest-prefix* | *dest/dest-prefix* | **any** }	目的IPv6地址信息	指定IPv6 ACL规则的目的IPv6地址信息	*dest*：目的IPv6地址 *dest-prefix*：前缀长度，取值范围1～128 **any**：任意目的IPv6地址
dscp *dscp*	报文优先级	DSCP优先级	*dscp*：用数字表示时，取值范围为0～63；用名称表示时，可选取**af11**（10）、**af12**（12）、**af13**（14）、**af21**（18）、**af22**（20）、**af23**（22）、**af31**（26）、**af32**（28）、**af33**（30）、**af41**（34）、**af42**（36）、**af43**（38）、**cs1**（8）、**cs2**（16）、**cs3**（24）、**cs4**（32）、**cs5**（40）、**cs6**（48）、**cs7**（56）、**default**（0）或**ef**（46）
flow-label *flow-label-value*	流标签字段	指定IPv6基本报文头中流标签字段的值	*flow-label-value*：流标签字段的值，取值范围为0～1048575
fragment	分片信息	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，则表示该规则对非分片报文和分片报文均有效
time-range *time-range-name*	时间段信息	指定规则生效的时间段	*time-range-name*：时间段的名称，为1～32个字符的字符串，不区分大小写，必须以英文字母a～z或A～Z开头

当*protocol*为**tcp**（6）或**udp**（17）时，用户还可配置如 表 1-11 所示的规则信息参数。

表1-11 TCP/UDP 特有的规则信息参数

参数	类别	作用	说明
source-port *operator port1* [*port2*]	源端口	定义TCP/UDP报文的源端口信息	*operator*：操作符，取值可以为**lt**（小于）、**gt**（大于）、**eq**（等于）、**neq**（不等于）或者**range**（在范围内，包括边界值）。只有**range**操作符需要两个端口号做操作数，其它操作符只需要一个端口号做操作数 *port1*/*port2*：TCP或UDP的端口号，用数字表示时，取值范围为0～65535；用名称表示时，TCP端口号可选取**chargen**（19）、**bgp**（179）、**cmd**（514）、**daytime**（13）、**discard**（9）、**domain**（53）、**echo**（7）、**exec**（512）、**finger**（79）、**ftp**（21）、**ftp-data**（20）、**gopher**（70）、**hostname**（101）、**irc**（194）、**klogin**（543）、**kshell**（544）、**login**（513）、**lpd**（515）、**nntp**（119）、**pop2**（109）、**pop3**（110）、**smtp**（25）、**sunrpc**（111）、**tacacs**（49）、**talk**（517）、**telnet**（23）、**time**（37）、**uucp**（540）、**whois**（43）或**www**（80）；UDP端口号可选取**biff**（512）、**bootpc**（68）、**bootps**（67）、**discard**（9）、**dns**（53）、**dnsix**（90）、**echo**（7）、**mobilip-ag**（434）、**mobilip-mn**（435）、**nameserver**（42）、**netbios-dgm**（138）、**netbios-ns**（137）、**netbios-ssn**（139）、**ntp**（123）、**rip**（520）、**snmp**（161）、**snmptrap**（162）、**sunrpc**（111）、**syslog**（514）、**tacacs-ds**（65）、**talk**（517）、**tftp**（69）、**time**（37）、**who**（513）或**xdmcp**（177）
destination-port *operator port1* [*port2*]	目的端口	定义TCP/UDP报文的目的端口信息	
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	TCP报文标识	定义对携带不同标志位（包括ACK、FIN、PSH、RST、SYN和URG六种）的TCP报文的处理规则	TCP协议特有的参数。表示匹配携带不同标志位的TCP报文，各*value*的取值可为0或1（0表示不携带此标志位，1表示携带此标志位） 如果在一条规则中设置了多个TCP标志位的匹配值，则这些匹配条件之间的关系为“与”
established	TCP连接建立标识	定义对TCP连接报文的处理规则	该参数用于定义TCP报文中ACK或RST标志位为1的报文

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

表1-12 ICMPv6 特有的规则信息参数

参数	类别	作用	说明
icmpv6-type { *icmpv6-type* *icmpv6-code* | *icmpv6-message* }	ICMPv6报文的消息类型和消息码信息	指定规则的ICMPv6报文的消息类型和消息码信息	*icmpv6-type*：ICMPv6消息类型，取值范围为0～255 *icmpv6-code*：ICMPv6的消息码，取值范围为0～255 *icmpv6-message*：ICMPv6消息的名称。可以输入的ICMPv6消息名称，及其与消息类型和消息码的对应关系如表1-13所示

表1-13 ICMPv6 消息名称与消息类型和消息码的对应关系

名称	ICMPv6 TYPE	ICMPv6 CODE
redirect	Type=137	Code=0
echo-request	Type=128	Code=0
echo-reply	Type=129	Code=0
err-Header-field	Type=4	Code=0
frag-time-exceeded	Type=3	Code=1

名称	ICMPv6 TYPE	ICMPv6 CODE
hop-limit-exceeded	Type=3	Code=0
host-admin-prohib	Type=1	Code=1
host-unreachable	Type=1	Code=3
neighbor-advertisement	Type=136	Code=0
neighbor-solicitation	Type=135	Code=0
network-unreachable	Type=1	Code=0
packet-too-big	Type=2	Code=0
port-unreachable	Type=1	Code=4
router-advertisement	Type=134	Code=0
router-solicitation	Type=133	Code=0
unknown-ipv6-opt	Type=4	Code=2
unknown-next-hdr	Type=4	Code=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**、**display ipv6 acl** 和 **step**。

说明

当 IPv6 高级 ACL 被 QoS 策略引用对报文进行流分类时，不支持配置 **flow-label**、**fragment** 参数。

【举例】

为 IPv6 高级 ACL 3000 创建一条规则，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 TCP 连接。

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

1.1.21 rule (IPv6 basic ACL view)

【命令】

rule [*rule-id*] { **deny** | **permit** } [**fragment** | **source** { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* **| any** } | **time-range** *time-range-name*] *

undo rule *rule-id* [**fragment** | **source** | **time-range**] *

【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。

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，则表示该规则对非分片报文和分片报文均有效。

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。

【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**、**display ipv6 acl** 和 **step**。

【举例】

为 IPv6 基本 ACL 2000 创建一条规则，拒绝源地址为 FE80:5060::101/128 的报文。

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule deny source fe80:5060::101/128
```

1.1.22 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 命令用来定义配置规则的描述信息。**undo rule comment** 命令用来删除规则的描述信息。

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 GE 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 GE 1/0/1.
```

1.1.23 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/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 的这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。

1.1.24 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
```

1.1.25 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。
- 使用同一名称可以配置多条不同的时间段，以达到这样的效果：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，再取二者的交集作为最终生效的时间范围。
- 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 月和 6 月内每周一的 10 点到 12 点以及每周三的 14 到 16 点。

```
<Sysname> system-view
[Sysname] time-range t4 10:0 to 12:0 1 from 0:0 1/1/2010 to 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 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 配置”。

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 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

字段	描述
Rule	分类规则

1.1.2 if-match

【命令】

if-match *match-criteria*

undo if-match *match-criteria*

undo if-match acl [**ipv6**] { *acl-number* | **name** *acl-name* } [**update acl** [**ipv6**] { *acl-number* | **name** *acl-name* }]

【视图】

类视图

【缺省级别】

2：系统级

【参数】

match-criteria：类的匹配规则，具体情况如 表 1-2 所示。

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

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

表1-2 匹配规则

取值	描述
acl [**ipv6**] { *acl-number* | **name** *acl-name* }	定义匹配ACL的规则 *acl-number*是ACL的序号，IPv4 ACL序号的取值范围是2000～3999，IPv6 ACL序号的取值范围是2000～3999，二层ACL序号的取值范围是4000～4999 *acl-name* 是 ACL 的名称，为 1～32 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，ACL 的名称不可以使用英文单词 all
any	定义匹配所有报文的规则
customer-dot1p *8021p-list*	定义匹配用户网络 802.1p 优先级的规则，*8021p-list* 为 CoS 取值的列表，最多可以输入 8 个 CoS 取值，用空格隔开，CoS 的取值范围为 0～7
customer-vlan-id *vlan-id-list*	定义匹配用户网络 VLAN ID 的规则，*vlan-id-list* 为 VLAN ID 的列表，形式可以为 *vlan-id* **to** *vlan-id*，也可以输入多个不连续的 VLAN ID，用空格隔开，设备最多允许用户同时指定 8 个 VLAN ID；VLAN ID 的取值范围为 1～4094
destination-mac *mac-address*	定义匹配目的 MAC 地址的规则
dscp *dscp-list*	定义匹配DSCP的规则，*dscp-list*为DSCP取值的列表，最多可以输入 8 个DSCP取值，用空格隔开，DSCP的取值范围为 0～63 或 表 1-4 中的关键字
ip-precedence *ip-precedence-list*	定义匹配 IP 优先级的规则，*ip-precedence-list* 为 IP 优先级取值的列表，最多可以输入 8 个 IP 优先级取值，用空格隔开，IP 优先级的取值范围为 0～7
protocol *protocol-name*	定义匹配协议的规则，*protocol-name* 取值为 IP 或 IPv6

取值	描述
service-dot1p *8021p-list*	定义匹配运营商网络 802.1p 优先级的规则，*8021p-list* 为 CoS 取值的列表，最多可以输入 8 个 CoS 取值，用空格隔开，CoS 的取值范围为 0～7
service-vlan-id *vlan-id-list*	定义匹配运营商网络 VLAN ID 的规则，*vlan-id-list* 为 VLAN ID 的列表，形式可以为 *vlan-id* **to** *vlan-id*，也可以输入多个不连续的 VLAN ID，用空格隔开，设备最多允许用户同时指定 8 个 VLAN ID；VLAN ID 的取值范围为 1～4094
source-mac *mac-address*	定义匹配源 MAC 地址的规则

说明

如果流分类中各规则之间的逻辑关系为 **and**，在定义匹配规则时，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）

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。

说明

当一个流分类中规则之间的逻辑关系为 **and** 时：

- 在一个流分类中，不能同时配置匹配 DSCP 优先级和匹配 IP 优先级的规则。
- 如果已经存在匹配 DSCP 优先级或匹配 IP 优先级的规则，则在指定匹配协议的规则时，只能匹配 IP 协议，不能匹配 IPv6 协议。

【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 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。

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
```

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

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

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 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 配置”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

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

【描述】

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

【举例】

显示配置的用户自定义的流行为信息。

```
<Sysname> display traffic behavior user-defined
User Defined Behavior Information:
  Behavior: test
    Filter enable: permit
  Behavior: USER1
    Marking:
      Remark IP Precedence 3
    Nesting:
      Nest Top-Most Vlan-ID  1000
  Behavior: USER2
    Redirect enable:
        Redirect type: interface
        Redirect destination: GigabitEthernet1/0/1
```

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

字段	描述
User Defined Behavior Information	用户自定义流行为的信息
Behavior	行为的名字及其内容，内容可以有多种类型
Marking	重标记的相关信息
Remark	重标记的类型。可支持的类型有DSCP、IP precedence、dot1p COS、local precedence等类型，相关类型描述请参考1.2 定义流行为的命令
Filter enable	流量过滤相关信息。过滤功能可以配置允许（permit）和阻止（deny）两种方式
Nesting	插入报文VLAN tag相关配置信息
Nest Top-Most Vlan-ID	插入运营商VLAN，具体描述可以参考命令**nest**
Redirect enable	流量重定向相关信息
Redirect type	重定向类型，目前支持重定向到端口
Redirect destination	重定向的目的，及端口类型和端口编号

1.2.2 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
```

1.2.3 redirect

【命令】

redirect interface *interface-type interface-number*

undo redirect interface *interface-type interface-number*

【视图】

流行为视图

【缺省级别】

2：系统级

【参数】

interface：重定向到指定的端口。

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

【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。

【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
```

1.2.4 remark dot1p

【命令】

remark dot1p *8021p*

undo remark dot1p

【视图】

流行为视图

【缺省级别】

2：系统级

【参数】

8021p：标记的 802.1p 优先级，取值范围为 0～7。

【描述】

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

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

【举例】

配置标记报文的 802.1p 优先级值为 2。

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

1.2.5 remark dscp

【命令】

remark dscp *dscp-value*

undo remark dscp

【视图】

流行为视图

【缺省级别】

2：系统级

【参数】

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

表1-4 DSCP 关键字与值的对应表

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

【描述】

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

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

【举例】

配置标记报文的 DSCP 值为 6。

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

1.2.6 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
```

1.2.7 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。

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
```

1.2.8 remark service-vlan-id

【命令】

remark service-vlan-id *vlan-id*

undo remark service-vlan-id

【视图】

流行为视图

【缺省级别】

2：系统级

【参数】

vlan-id：表示重标记报文运营商 VLAN 的编号，取值范围为 1～4094。

【描述】

remark service-vlan-id 命令用来配置重标记运营商的 VLAN ID。**undo remark service-vlan-id** 命令用来取消重标记运营商的 VLAN ID。

【举例】

在流行为 b1 上配置重标记报文运营商的 VLAN ID 为 VLAN 222。

```
<Sysname> system-view
[Sysname] traffic behavior b1
[Sysname-behavior-b1] remark service-vlan-id 222
```

1.2.9 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*

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。

【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。

相关配置可参考命令 **qos policy**。

【举例】

在策略 user1 中为类 database 指定采用流行为 test。

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

1.3.2 display qos policy

【命令】

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

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

user-defined：用户定义策略。

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

tcl-name：策略中的类名。

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

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: USER1
    Marking:
      Remark IP Precedence 3
```

表1-5 display qos policy 命令显示信息描述表

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

1.3.3 display qos policy global

【命令】

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

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

inbound：显示设备所有端口入方向应用的 QoS 策略信息。

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 配置”。

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。

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 inbound

  Direction: Inbound

  Policy: 1
   Classifier: 1
     Operator: AND
     Rule(s) : -none-
     Behavior: 1
      Marking:
        Remark dot1p COS 1
      Marking:
        Remark Service VLAN ID 2
      Redirect enable:
        Redirect type: interface
        Redirect destination: GigabitEthernet1/0/1
   Classifier: 54 (Failed)
     Operator: AND
     Rule(s) : -none-
     Behavior: 8
      -none-
```

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

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

字段	描述
Behavior	流行为的名称及其内容，内容可以有多种类型

1.3.4 display qos policy interface

【命令】

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

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

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

inbound：显示对端口接收到的报文应用的 QoS 策略信息。

|：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 配置”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

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

【描述】

display qos policy interface 命令用来显示指定端口或所有端口上 QoS 策略的配置信息和运行情况。

【举例】

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

```
<Sysname> display qos policy interface gigabitethernet 1/0/1

  Interface: GigabitEthernet1/0/1

  Direction: Inbound
  Policy: 1
   Classifier: 1
     Operator: OR
     Rule(s) : -none-
     Behavior: 1
      Marking:
        Remark dot1p COS 1
      Marking:
        Remark Service VLAN ID 2
      Redirect enable:
        Redirect type: interface
        Redirect destination: GigabitEthernet1/0/2

   Classifier: 54 (Failed)
```

```
Operator: AND
Rule(s) : -none-
Behavior: 8
 -none-
```

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

字段	描述
Interface	端口名，由端口类型和端口编号结合在一起组成。
Direction	Policy应用在端口的方向
Policy	应用到端口上的策略的名字
Classifier	策略里分类规则以及对应的配置信息。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端口上正常应用；
Operator	同一个类中多条分类规则的逻辑关系
Rule(s)	类的分类规则
Behavior	策略里行为的名字及配置信息，参见流行为的相关命令

1.3.5 display qos vlan-policy

【命令】

display qos vlan-policy { **name** *policy-name* | **vlan** [*vlan-id*] } [**slot** *slot-number*] [**inbound**] [**|** { **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。

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 配置”。

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。

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

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

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

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

显示 VLAN 2 的 QoS 策略信息。

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

  Vlan 2

  Direction: Inbound
  Policy: 1
   Classifier: 1
     Operator: OR
     Rule(s) : -none-
     Behavior: 1
      Marking:
        Remark dot1p COS 1
      Marking:
        Remark Service VLAN ID 2
      Redirect enable:
        Redirect type: interface
        Redirect destination: GigabitEthernet1/0/2
   Classifier: 54
     Operator: AND
     Rule(s) : -none-
     Behavior: 8
      -none-
```

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

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

字段	描述
Operator	分类规则之间的逻辑关系
Rule(s)	分类规则
Behavior	流行为的名称及其内容，内容可以有多种类型

1.3.6 qos apply policy (interface view, port group view)

【命令】

qos apply policy *policy-name* **inbound**

undo qos apply policy [*policy-name*] **inbound**

【视图】

以太网端口视图/端口组视图

【缺省级别】

2：系统级

【参数】

inbound：入方向。

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

【描述】

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

在以太网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】

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

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

1.3.7 qos apply policy (user-profile view)

【命令】

qos apply policy *policy-name* **inbound**

undo qos apply policy [*policy-name*] **inbound**

【视图】

user-profile 视图

【缺省级别】

2：系统级

【参数】

inbound：对上线用户接收到的报文应用策略。

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** 和 **filter** 两种动作。
- user-profile 视图下应用的策略不能为空策略。

【举例】

对上线用户 user 接收的报文应用策略 test（该策略已经建立）。

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

1.3.8 qos apply policy global

【命令】

qos apply policy *policy-name* **global inbound**

undo qos apply policy [*policy-name*] **global inbound**

【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报文应用 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
```

1.3.9 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** 和 **qos apply policy**。

【举例】

定义一个名为 user1 的策略。

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

1.3.10 qos vlan-policy

【命令】

qos vlan-policy *policy-name* **vlan** *vlan-id-list* **inbound**

undo qos vlan-policy [*policy-name*] **vlan** *vlan-id-list* **inbound**

【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。

【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
```

1.3.11 reset qos policy global

【命令】

reset qos policy global [**inbound**]

【视图】

用户视图

【缺省级别】

1：监控级

【参数】

inbound：入方向。

【描述】

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

【举例】

清除全局入方向应用的 QoS 策略的统计信息。

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

1.3.12 reset qos vlan-policy

【命令】

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

【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。

【描述】

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

【举例】

清除 VLAN 2 应用的 QoS 策略的统计信息。

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

2 优先级映射配置命令

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-dot1p** | **dot1p-dscp** | **dot1p-lp** | **dscp-dot1p** | **dscp-dscp** | **dscp-lp**]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

dot1p-dot1p：802.1p 优先级到 802.1p 优先级映射表。

dot1p-dscp：802.1p 优先级到 DSCP 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-dscp：DSCP 到 DSCP 映射表。

dscp-lp：DSCP 到本地优先级映射表。

|：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 配置”。

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
```

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-dot1p** | **dot1p-dscp** | **dot1p-lp** | **dscp-dot1p** | **dscp-dscp** | **dscp-lp** }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

dot1p-dot1p：802.1p 优先级到 802.1p 优先级映射表。

dot1p-dscp：802.1p 优先级到 DSCP 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-dscp：DSCP 到 DSCP 映射表。

dscp-lp：DSCP 到本地优先级映射表。

【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 优先级到本地优先级映射表视图。

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

2.2 端口优先级配置命令

2.2.1 qos priority

【命令】

qos priority *priority-value*

undo qos priority

【视图】

以太网端口视图/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。

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

端口优先级的缺省值为 0。

【举例】

配置以太网端口 GigabitEthernet1/0/1 的端口优先级为 2。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos priority 2
```

2.3 端口优先级信任模式配置命令

2.3.1 display qos trust interface

【命令】

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

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

interface-type interface-number：指定的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 配置”。

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。

如果不指定端口，本命令将显示所有端口的端口优先级信任模式信息。

【举例】

显示当前配置的端口优先级信任模式信息。

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

表2-2 display qos trust 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构成
Port priority trust information	端口优先级信任信息
Port priority	端口优先级
Port priority trust type	优先级信任模式： • dscp 表示信任报文的 DSCP 优先级 • dot1p 表示信任报文的 802.1p 优先级 • untrust 表示不信任报文的优先级

2.3.2 qos trust

【命令】

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

undo qos trust

【视图】

以太网端口视图/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，信任模式为信任接收端口的优先级。

在以太网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】

在以太网端口 GigabitEthernet1/0/1 上配置优先级信任模式为信任报文自带的 802.1p 优先级。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos trust dot1p
```

3 端口限速配置命令

3.1 端口限速配置命令

3.1.1 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 配置”。

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 命令用来显示某个端口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 1280 (kbps)
Interface: GigabitEthernet1/0/2
Direction: Inbound
 CIR 6400 (kbps)
```

表3-1 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是入方向还是出方向
CIR	承诺信息速率，单位为kbps

3.1.2 qos lr

【命令】

qos lr { **inbound** | **outbound** } **cir** *committed-information-rate*

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

【视图】

以太网端口视图/端口组视图

【缺省级别】

2：系统级

【参数】

inbound：对端口接收的数据流进行限速。

outbound：对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，取值范围为 64～1000000 且必须是 64 的整数倍。

【描述】

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

在以太网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】

对端口 GigabitEthernet1/0/1 发出的报文进行限速，限制速率为 256kbps。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos lr outbound cir 256
```

4 拥塞管理配置命令

4.1 拥塞管理配置命令

4.1.1 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 配置”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

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

【描述】

display qos wrr interface 命令用来显示端口的队列配置情况。

如不指定端口，本命令将显示所有端口的 WRR 队列配置情况。

相关配置可参考命令 **qos wrr**。

【举例】

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

```
<Sysname> display qos wrr interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
 Output queue: Weighted round robin queue
Queue ID    Group    Weight
-------------------------------------
   0         sp       N/A
   1         1        10
   2         sp       N/A
   3         2        30
```

表4-1 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

字段	描述
Group	分组号，说明队列属于哪一个分组，缺省情况下，队列所属的分组为sp
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

4.1.2 qos wrr

【命令】

qos wrr *queue-id* **group** { *group-id* **weight** *queue-weight* | **sp** }

undo qos wrr [*queue-id* **group** { *group-id* **weight** | **sp** }]

【视图】

以太网端口视图/端口组视图

【缺省级别】

2：系统级

【参数】

wrr *queue-id*：队列编号，取值范围为 0～3。

group-id：将队列划入 WRR 调度组，取值范围为 1～2。

weight *queue-weight*：队列的权重，取值范围为 1～100。

sp：将队列划入 SP 调度组。

【描述】

qos wrr 命令用来在端口或端口组上配置 WRR 或 SP+WRR 调度算法。**undo qos wrr** 命令用来恢复缺省情况。

缺省情况下，采用 SP（严格优先级）调度算法。

本系列以太网交换机的端口支持 4 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，实现 SP+WRR 的调度功能。

【举例】

配置端口 GigabitEthernet 1/0/1 使用 SP+WRR 队列调度算法，0 队列属于 SP 调度组，1 队列属于 WRR 调度组 1，权重为 20，2、3 队列属于 WRR 调度组 2，权重分别为 10、50。

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wrr 0 group sp
[Sysname-GigabitEthernet1/0/1] qos wrr 1 group 1 weight 20
[Sysname-GigabitEthernet1/0/1] qos wrr 2 group 2 weight 10
[Sysname-GigabitEthernet1/0/1] qos wrr 3 group 2 weight 50
```

5 Burst功能配置命令

5.1 Burst功能配置命令

5.1.1 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 命令用来使能 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。

在下列情况下，Burst 功能可以提供更好的报文缓存功能和流量转发性能：

- 广播或者组播报文流量密集，瞬间突发大流量的网络环境中；
- 报文从高速链路进入交换机，由低速链路转发出去；或者报文从相同速率的多个端口同时进入交换机，由一个相同速率的端口转发出去。

用户可以通过开启 Burst 功能，降低设备在上述特定环境中的报文丢包率，提高对报文的处理能力。

【举例】

使能 Burst 功能。

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