

H3C S5130S-SI[LI]&S5120V2-SI[LI]&S5110V2-SI& S5000V3-EI&S5000E-X&S3100V3-SI 系列以太网交换机

ACL 和 QoS 命令参考

新华三技术有限公司
<http://www.h3c.com>

资料版本：6W103-20190822
产品版本：Release 612x 系列

Copyright © 2019 新华三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。

除新华三技术有限公司的商标外，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。

前言

本命令参考主要介绍 ACL、QoS、数据缓冲区和时间段等功能的命令。
前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [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

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。
<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 ... }	表示从多个选项中仅选取一个。
[x y ...]	表示从多个选项选取一个或者不选。
{ x y ... } *	表示从多个选项中至少选取一个。
[x y ...] *	表示从多个选项选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1~n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

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

3. 各类标志

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

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

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

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

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

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail: info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 ACL	1-1
1.1 ACL配置命令	1-1
1.1.1 acl	1-1
1.1.2 acl copy	1-3
1.1.3 acl logging interval	1-4
1.1.4 acl trap interval	1-5
1.1.5 description	1-6
1.1.6 display acl	1-7
1.1.7 display packet-filter	1-8
1.1.8 display packet-filter statistics	1-9
1.1.9 display packet-filter statistics sum	1-12
1.1.10 display packet-filter verbose	1-13
1.1.11 display qos-acl resource	1-15
1.1.12 packet-filter	1-16
1.1.13 packet-filter default deny	1-18
1.1.14 reset packet-filter statistics	1-19
1.1.15 rule (IPv4 advanced ACL view)	1-19
1.1.16 rule (IPv4 basic ACL view)	1-24
1.1.17 rule (IPv6 advanced ACL view)	1-26
1.1.18 rule (IPv6 basic ACL view)	1-31
1.1.19 rule (Layer 2 ACL view)	1-33
1.1.20 rule comment	1-35
1.1.21 step	1-36

1 ACL

1.1 ACL配置命令

1.1.1 acl

acl 命令用来创建 ACL，并进入 ACL 视图。如果指定的 ACL 已存在，则直接进入 ACL 视图。

undo acl 命令用来删除指定或全部 ACL。

【命令】

命令形式一

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

```
undo acl [ ipv6 ] { all | name acl-name | number acl-number }
```

命令形式二

```
acl [ ipv6 ] { advanced | basic } { acl-number | name acl-name } [ match-order { auto | config } ]
```

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

```
undo acl [ ipv6 ] { all | { advanced | basic } { acl-number | name acl-name } }
```

```
undo acl mac { all | acl-number | name acl-name }
```

【缺省情况】

不存在 ACL。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv6: 指定 ACL 类型为 IPv6 ACL。如果未指定本参数，则表示 IPv4 ACL。

basic: 指定创建基本 ACL。

advanced: 指定创建高级 ACL。

mac: 指定创建二层 ACL。

number *acl-number*: 指定 ACL 的编号。

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: 表示基本 ACL。
- 3000~3999: 表示高级 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: 指定类型中全部 ACL。

【使用指导】

指定 ACL 编号创建的 ACL，可以通过如下命令进入其视图：

- **acl [ipv6] number acl-number;**
- **acl { [ipv6] { advanced | basic } | mac } acl-number。**

通过 **acl [ipv6] number acl-number name acl-name** 命令创建的 ACL，可以通过如下命令进入其视图：

- **acl [ipv6] name acl-name,** 本命令仅支持进入已创建的基本 ACL 或高级 ACL 视图；
- **acl [ipv6] number acl-number [name acl-name];**
- **acl { [ipv6] { advanced | basic } | mac } name acl-name。**

通过 **acl { [ipv6] { advanced | basic } | mac } name acl-name** 命令创建的 ACL，只能通过如下命令进入其视图：

- **acl [ipv6] name acl-name,** 本命令仅支持进入已创建的基本 ACL 或高级 ACL 视图；
- **acl { [ipv6] { advanced | basic } | mac } name acl-name。**

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。

如果 ACL 规则的匹配项中包含了除 IP 五元组（源 IP 地址、源端口号、目的 IP 地址、目的端口号、传输层协议）、ICMP 报文或 ICMPv6 报文的类型和消息码信息、日志操作和时间段之外的其它匹配项，则设备转发 ACL 匹配的这类报文时会启用慢转发流程。慢转发时设备会将报文上送控制平面，计算报文相应的表项信息。执行慢转发流程时，设备的转发能力将会有所降低。

【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 basic 2000
[Sysname-acl-ipv4-basic-2000]
```

创建一个 IPv4 基本 ACL，指定其名称为 flow，并进入其视图。

```
<Sysname> system-view
[Sysname] acl basic name flow
[Sysname-acl-ipv4-basic-flow]
```

创建一个编号为 3000 的 IPv4 高级 ACL，并进入其视图。

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000]
```

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 basic 2000
[Sysname-acl-ipv6-basic-2000]
# 创建一个 IPv6 基本 ACL，其名称为 flow，并进入其视图。
<Sysname> system-view
[Sysname] acl ipv6 basic name flow
[Sysname-acl-ipv6-basic-flow]
# 创建一个 IPv6 高级 ACL，其名称为 abc，并进入其视图。
<Sysname> system-view
[Sysname] acl ipv6 advanced name abc
[Sysname-acl-ipv6-adv-abc]
# 创建一个编号为 4000 的二层 ACL，并进入其视图。
<Sysname> system-view
[Sysname] acl mac 4000
[Sysname-acl-mac-4000]
# 创建一个二层 ACL，其名称为 flow，并进入其视图。
<Sysname> system-view
[Sysname] acl mac name flow
[Sysname-acl-mac-flow]

```

【相关命令】

- **display acl**

1.1.2 acl copy

acl copy 命令用来复制并生成一个新的 ACL。

【命令】

```

acl [ ipv6 | mac ] copy { source-acl-number | name source-acl-name } to
{ dest-acl-number | name dest-acl-name }

```

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv6: 指定 ACL 类型为 IPv6 ACL。

mac: 指定 ACL 类型为二层 ACL。

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: 表示基本 ACL。
- 3000~3999: 表示高级 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。

dest-acl-number: 指定目的 ACL 的编号, 该 ACL 必须不存在。本参数的取值范围及其代表的 ACL 类型如下:

- 2000~2999: 表示基本 ACL。
- 3000~3999: 表示高级 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**。

【使用指导】

目的 ACL 的类型要与源 ACL 的类型相同。

除了 ACL 的编号或名称不同外, 新生成的 ACL (即目的 ACL) 的匹配顺序、规则匹配软件统计功能的开启情况、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。

若未指定 **ipv6**、**mac** 参数, 则表示 IPv4 ACL。

【举例】

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

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

通过复制已存在的 IPv4 基本 ACL test, 来生成名为 paste 的同类型 ACL。

```
<Sysname> system-view
[Sysname] acl copy name test to name paste
```

1.1.3 acl logging interval

acl logging interval 命令用来配置报文过滤日志信息的生成与发送周期。

undo acl logging interval 命令用来恢复缺省情况。

【命令】

```
acl logging interval interval
undo acl logging interval
```

【缺省情况】

报文过滤日志信息的生成与发送周期为 0 分钟, 即不记录报文过滤的日志。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval: 报文过滤日志信息的生成与发送周期, 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。

【使用指导】

系统只支持对应用 IPv4 基本 ACL、IPv4 高级 ACL、IPv6 基本 ACL 或 IPv6 高级 ACL 进行报文过滤的报文过滤日志信息进行记录，且在上述 ACL 中配置规则时必须指定 **logging** 参数。

报文过滤日志的生成与发送周期起始于报文过滤中 ACL 匹配数据流的第一个数据包，报文过滤日志包括周期内被匹配的报文数量以及所使用的 ACL 规则。在一个周期内：

- 对于规则匹配数据流的第一个数据包，设备会立即生成报文过滤日志并发送到信息中心；
- 对于规则匹配数据流的其他数据包，设备将在周期结束后生成报文过滤日志并发送到信息中心。

有关信息中心的详细介绍请参见“网络管理和监控配置指导”中的“信息中心”。

【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 interval 10
```

【相关命令】

- **rule** (IPv4 advanced ACL view)
- **rule** (IPv4 basic ACL view)
- **rule** (IPv6 advanced ACL view)
- **rule** (IPv6 basic ACL view)

1.1.4 acl trap interval

acl trap interval 命令用来配置报文过滤告警信息的生成与发送周期。

undo acl trap interval 命令用来恢复缺省情况。

【命令】

```
acl trap interval interval  
undo acl trap interval
```

【缺省情况】

报文过滤告警信息的生成与发送周期为 0 分钟，即不记录报文过滤的告警信息。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval：报文过滤告警信息的生成与发送周期，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。

【使用指导】

系统只支持对应用 IPv4 基本 ACL、IPv4 高级 ACL、IPv6 基本 ACL 或 IPv6 高级 ACL 进行报文过滤的报文过滤告警信息进行记录，且在上述 ACL 中配置规则时必须指定 **logging** 参数。

报文过滤告警信息的生成与发送周期起始于报文过滤中 **ACL** 匹配数据流的第一个数据包, 报文过滤告警信息包括周期内被匹配的报文数量以及所使用的 **ACL** 规则。在一个周期内:

- 对于规则匹配数据流的第一个数据包, 设备会立即生成报文过滤告警信息并发送到 **SNMP** 模块;
- 对于规则匹配数据流的其他数据包, 设备将在周期结束后生成报文过滤告警信息并发送到 **SNMP** 模块。

有关 **SNMP** 的详细介绍, 请参见“网络管理和监控配置指导”中的“**SNMP**”。

【举例】

配置 IPv4 报文过滤告警信息的生成与发送周期为 10 分钟。

```
<Sysname> system-view
[Sysname] acl trap interval 10
```

【相关命令】

- **rule** (IPv4 advanced ACL view)
- **rule** (IPv4 basic ACL view)
- **rule** (IPv6 advanced ACL view)
- **rule** (IPv6 basic ACL view)

1.1.5 description

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。

【命令】

```
description text
undo description
```

【缺省情况】

ACL 没有任何描述信息。

【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

【缺省用户角色】

network-admin

【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。

【举例】

为 IPv4 基本 **ACL** 2000 配置描述信息。

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] description This is an IPv4 basic ACL.
```

【相关命令】

- **display acl**

1.1.6 display acl

display acl 命令用来显示 ACL 的配置和运行情况。

【命令】

display acl [**ipv6** | **mac**] { *acl-number* | **all** | **name** *acl-name* }

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

ipv6: 指定 ACL 类型为 IPv6 ACL。

mac: 指定 ACL 类型为二层 ACL。

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

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

all: 显示指定类型中全部 ACL 的配置和运行情况。

name *acl-name*: 显示指定名称的 ACL 的配置和运行情况。*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

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。

如果未指定 **ipv6**、**mac** 参数，则表示 IPv4 ACL。

【举例】

显示 IPv4 基本 ACL 2001 的配置和运行情况。

```
<Sysname> display acl 2001
Basic IPv4 ACL 2001, 1 rule, match-order is auto,
This is an IPv4 basic ACL.
ACL's step is 5, start ID is 0
rule 5 permit source 1.1.1.1 0
rule 5 comment This rule is used on GigabitEthernet1/0/1.
```

表1-1 display acl 命令显示信息描述表

字段	描述
Basic IPv4 ACL 2001	该ACL的类型和编号
1 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）
This is an IPv4 basic ACL.	该ACL的描述信息
ACL's step is 5	该ACL的规则编号的步长值为5
start ID is 0	该ACL的规则编号的起始值为0
rule 5 permit source 1.1.1.1 0	规则5的具体内容，源地址为具体地址
rule 5 comment This rule is used on GigabitEthernet1/0/1.	规则5的描述信息

1.1.7 display packet-filter

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

【命令】

```
display packet-filter interface [ interface-type interface-number ]
[ inbound | outbound ] [ slot slot-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface [*interface-type interface-number*]: 显示指定接口上 ACL 在报文过滤中的应用情况。*interface-type interface-number* 表示接口类型和接口编号。若未指定接口类型和接口编号，将显示所有接口上 ACL 在报文过滤中的应用情况。当接口类型为以太网接口时，不需要指定 **slot** 参数。

inbound: 显示入方向上 ACL 在报文过滤中的应用情况。

outbound: 显示出方向上 ACL 在报文过滤中的应用情况。

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

【使用指导】

如果未指定 **inbound** 和 **outbound** 参数，将同时显示出、入方向上 ACL 在报文过滤中的应用情况。

【举例】

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

```
<Sysname> display packet-filter interface gigabitethernet 1/0/1 inbound
Interface: GigabitEthernet1/0/1
Inbound policy:
  IPv4 ACL 2001
  IPv6 ACL 2002 (Failed)
  MAC ACL 4003
```

表1-2 display packet-filter 命令显示信息描述表

字段	描述
Interface	ACL在指定接口上的应用情况
Inbound policy	ACL在入方向上的应用情况
Outbound policy	ACL在出方向上的应用情况
IPv4 ACL 2001	IPv4基本ACL 2001应用成功
IPv6 ACL 2002 (Failed)	IPv6基本ACL 2002应用失败
Hardware-count	规则匹配硬件统计功能应用成功
Hardware-count (Failed)	规则匹配硬件统计功能应用失败
IPv4 default action	报文过滤的缺省动作，包括： <ul style="list-style-type: none">• Deny: 报文过滤缺省动作为 Deny 应用成功• Deny (Failed): 报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit• Permit: 报文过滤缺省动作为 Permit
IPv6 default action	报文过滤的缺省动作，包括： <ul style="list-style-type: none">• Deny: 报文过滤缺省动作为 Deny 应用成功• Deny (Failed): 报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit• Permit: 报文过滤缺省动作为 Permit
MAC default action	报文过滤的缺省动作，包括： <ul style="list-style-type: none">• Deny: 报文过滤缺省动作为 Deny 应用成功• Deny (Failed): 报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit• Permit: 报文过滤缺省动作为 Permit

1.1.8 display packet-filter statistics

display packet-filter statistics 命令用来显示 ACL 在报文过滤中应用的统计信息。

【命令】

```
display packet-filter statistics interface interface-type interface-number
{ inbound | outbound } [ [ ipv6 | mac ] { acl-number | name acl-name } ] [ brief ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface *interface-type interface-number*: 显示指定接口上的统计信息。
interface-type interface-number 表示接口类型和接口编号。

inbound: 显示入方向上的统计信息。

outbound: 显示出方向上的统计信息。

ipv6: 指定 ACL 类型为 IPv6 ACL。

mac: 指定 ACL 类型为二层 ACL。

acl-number: 显示指定编号 ACL 在报文过滤中应用的统计信息。*acl-number* 表示 ACL 的编号, 取值范围及其代表的 ACL 类型如下:

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

name *acl-name*: 显示指定名称 ACL 在报文过滤中应用的统计信息。*acl-name* 表示 ACL 的名称, 为 1~63 个字符的字符串, 不区分大小写。

brief: 显示简要统计信息。

【使用指导】

如果未指定 *acl-number*、**name** *acl-name* 和 ACL 类型 (**ipv6**、**mac**) 参数, 将显示全部 ACL 在报文过滤中应用的统计信息。

如果未指定 **ipv6**、**mac** 参数, 则表示 IPv4 ACL。

【举例】

显示接口 GigabitEthernet1/0/1 入方向上全部 ACL 在报文过滤中应用的统计信息。

```
<Sysname> display packet-filter statistics interface gigabitethernet 1/0/1 inbound
Interface: GigabitEthernet1/0/1
Inbound policy:
IPv4 ACL 2001, Hardware-count
  From 2011-06-04 10:25:21 to 2011-06-04 10:35:57
  rule 0 permit source 2.2.2.2 0 (2 packets)
  rule 5 permit source 1.1.1.1 0 (Failed)
  Totally 2 packets permitted, 0 packets denied
  Totally 100% permitted, 0% denied

IPv6 ACL 2000

MAC ACL 4000
  rule 0 permit
```


表1-3 display packet-filter statistics 命令显示信息描述表

字段	描述
Interface	在指定接口上应用的统计信息
Inbound policy	在入方向上应用的统计信息
Outbound policy	在出方向上应用的统计信息
IPv4 ACL 2001	IPv4基本ACL 2001应用成功
IPv4 ACL 2002 (Failed)	IPv4基本ACL 2002应用失败
Hardware-count	规则匹配硬件统计功能应用成功
Hardware-count (Failed)	规则匹配硬件统计功能应用失败
From 2011-06-04 10:25:21 to 2011-06-04 10:35:57	硬件统计的起始和终止时间
2 packets	该规则匹配了2个包（当匹配的包个数为0时不显示本字段）
No resource	该规则对应的统计资源不足。在显示统计信息时，若该规则的统计资源不足，便会显示本字段
rule 5 permit source 1.1.1.1 0 (Failed)	规则5应用失败
Totally 2 packets permitted, 0 packets denied	该ACL允许和拒绝符合条件报文的个数
Totally 100% permitted, 0% denied	该ACL允许符合条件报文的通过率和拒绝符合条件报文的丢弃率
IPv4 default action	报文过滤的缺省动作，包括： <ul style="list-style-type: none"> Deny: 报文过滤缺省动作为 Deny 应用成功 Deny (Failed): 报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit Permit: 报文过滤缺省动作为 Permit
IPv6 default action	报文过滤的缺省动作，包括： <ul style="list-style-type: none"> Deny: 报文过滤缺省动作为 Deny 应用成功 Deny (Failed): 报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit Permit: 报文过滤缺省动作为 Permit
MAC default action	报文过滤的缺省动作，包括： <ul style="list-style-type: none"> Deny: 报文过滤缺省动作为 Deny 应用成功 Deny (Failed): 报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit Permit: 报文过滤缺省动作为 Permit

【相关命令】

- **reset packet-filter statistics**

1.1.9 display packet-filter statistics sum

display packet-filter statistics sum 命令用来显示 ACL 在报文过滤中应用的累加统计信息。

【命令】

```
display packet-filter statistics sum { inbound | outbound } [ ipv6 | mac ]  
{ acl-number | name acl-name } [ brief ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

inbound: 显示入方向上 ACL 在报文过滤中应用的累加统计信息。

outbound: 显示出方向上 ACL 在报文过滤中应用的累加统计信息。

ipv6: 指定 ACL 类型为 IPv6 ACL。

mac: 指定 ACL 类型为二层 ACL。

acl-number: 显示指定编号 ACL 在报文过滤中应用的累加统计信息。*acl-number* 表示 ACL 的编号，取值范围及其代表的 ACL 类型如下：

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

name acl-name: 显示指定名称 ACL 在报文过滤中应用的累加统计信息。*acl-name* 表示 ACL 的名称，为 1~63 个字符的字符串，不区分大小写。

brief: 显示 ACL 在报文过滤中应用的简要累加统计信息。

【使用指导】

如果未指定 **ipv6**、**mac** 参数，则表示 IPv4 ACL。

【举例】

显示入方向上 IPv4 基本 ACL 2001 在报文过滤中应用的累加统计信息。

```
<Sysname> display packet-filter statistics sum inbound 2001
```

Sum:

Inbound policy:

IPv4 ACL 2001

rule 0 permit source 2.2.2.2 0 (2 packets)

rule 5 permit source 1.1.1.1 0

Totally 2 packets permitted, 0 packets denied

Totally 100% permitted, 0% denied

显示入方向上 IPv4 基本 ACL 2000 在报文过滤中应用的简要累加统计信息。

```
<Sysname> display packet-filter statistics sum inbound 2000 brief
```

Sum:

```
Inbound policy:
IPv4 ACL 2000
Totally 2 packets permitted, 0 packets denied
Totally 100% permitted, 0% denied
```

表1-4 display packet-filter statistics sum 命令显示信息描述表

字段	描述
Sum	ACL在报文过滤中应用的累加统计信息
Inbound policy	ACL在入方向上应用的累加统计信息
Outbound policy	ACL在出方向上应用的累加统计信息
IPv4 ACL 2001	IPv4基本ACL 2001应用的累加统计信息
2 packets	该规则匹配了2个包（当匹配的包个数为0时不显示本字段）
Totally 2 packets permitted, 0 packets denied	该ACL允许和拒绝符合条件报文的个数
Totally 100% permitted, 0% denied	该ACL允许符合条件报文的通过率和拒绝符合条件报文的丢弃率

【相关命令】

- **reset packet-filter statistics**

1.1.10 display packet-filter verbose

display packet-filter verbose 命令用来显示 ACL 在报文过滤中的详细应用情况。

【命令】

```
display packet-filter verbose interface interface-type interface-number
{ inbound | outbound } [ [ ipv6 | mac ] { acl-number | name acl-name } ] [ slot
slot-number ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
```

【参数】

interface interface-type interface-number: 显示指定接口上 ACL 在报文过滤中的详细应用情况。*interface-type interface-number* 表示接口类型和接口编号。当接口类型为以太网接口时，不需要指定 **slot** 参数。

inbound: 显示入方向上 ACL 在报文过滤中的详细应用情况。

outbound: 显示出方向上 ACL 在报文过滤中的详细应用情况。

ipv6: 指定 ACL 类型为 IPv6 ACL。

mac: 指定 ACL 类型为二层 ACL。

acl-number: 显示指定编号 ACL 在报文过滤中的详细应用情况。*acl-number* 表示 ACL 的编号，取值范围及其代表的 ACL 类型如下：

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

name *acl-name*: 显示指定名称 ACL 在报文过滤中的详细应用情况。*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写。

slot *slot-number*: 显示指定成员设备上 ACL 在报文过滤中的详细应用情况，*slot-number* 表示设备在 IRF 中的成员编号。若未指定本参数，将显示主用设备上 ACL 在报文过滤中的详细应用情况。

【使用指导】

若未指定 *acl-number*、**name** *acl-name* 和 ACL 类型 (**ipv6**、**mac**) 参数，将显示全部 IPv4 ACL 在报文过滤中的详细应用情况。

如果未指定 **ipv6**、**mac** 参数，则表示 IPv4 ACL。

【举例】

```
# 显示接口 GigabitEthernet1/0/1 入方向上全部 ACL 在报文过滤中的详细应用情况。
<Sysname> display packet-filter verbose interface gigabitethernet 1/0/1 inbound
Interface: GigabitEthernet1/0/1
Inbound policy:
  IPv4 ACL 2001
    rule 0 permit
    rule 5 permit source 1.1.1.1 0 (Failed)

  IPv6 ACL 2000
    rule 0 permit

  MAC ACL 4000

  IPv4 default action: Deny

  IPv6 default action: Deny

  MAC default action: Deny
```

表1-5 display packet-filter verbose 命令显示信息描述表

字段	描述
Interface	ACL在指定接口上的详细应用情况
Inbound policy	ACL在入方向上的详细应用情况
Outbound policy	ACL在出方向上的详细应用情况
IPv4 ACL 2001	IPv4基本ACL 2001应用成功
IPv4 ACL 2002 (Failed)	IPv4基本ACL 2002应用失败

字段	描述
Hardware-count	规则匹配硬件统计功能应用成功
Hardware-count (Failed)	规则匹配硬件统计功能应用失败
rule 5 permit source 1.1.1.1 0 (Failed)	规则5应用失败
IPv4 default action	报文过滤的缺省动作，包括： <ul style="list-style-type: none"> Deny: 报文过滤缺省动作为 Deny 应用成功 Deny (Failed): 报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit Permit: 报文过滤缺省动作为 Permit
IPv6 default action	报文过滤的缺省动作，包括： <ul style="list-style-type: none"> Deny: 报文过滤缺省动作为 Deny 应用成功 Deny (Failed): 报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit Permit: 报文过滤缺省动作为 Permit
MAC default action	报文过滤的缺省动作，包括： <ul style="list-style-type: none"> Deny: 报文过滤缺省动作为 Deny 应用成功 Deny (Failed): 报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit Permit: 报文过滤缺省动作为 Permit

1.1.11 display qos-acl resource

display qos-acl resource 命令用来显示 QoS 和 ACL 资源的使用情况。

【命令】

display qos-acl resource [*slot slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

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

【使用指导】

如果指定的设备不支持统计 QoS 和 ACL 资源，将不会显示该设备上 QoS 和 ACL 资源的使用情况。设备 QoS 和 ACL 资源不足时会导致某些功能无法使用，例如报文过滤、登录设备、802.1X、MAC 地址认证等，如需使用该类应用，请预留相应的 QoS 和 ACL 资源。

【举例】

显示 QoS 和 ACL 资源的使用情况。

```
<Sysname> display qos-acl resource
```

```
Interfaces: GE1/0/1 to GE1/0/24, XGE1/0/51 to XGE1/0/52 (slot 1)
```

Type	Total	Reserved	Configured	Remaining	Usage
TTI ACL	256	0	0	256	0%
PCL ACL	512	16	0	496	3%
PCL Counter	656	14	0	642	2%
IPCL Meter	768	0	0	768	0%
EPCL Meter	128	0	0	128	0%

```
Interfaces: GE1/0/25 to GE1/0/48, XGE1/0/49 to XGE1/0/50 (slot 1)
```

Type	Total	Reserved	Configured	Remaining	Usage
TTI ACL	256	0	0	256	0%
PCL ACL	512	16	0	496	3%
PCL Counter	656	14	0	642	2%
IPCL Meter	768	0	0	768	0%
EPCL Meter	128	0	0	128	0%

表1-6 display qos-acl resource 命令显示信息描述表

字段	描述
Interfaces	资源对应的接口范围
Type	资源类型： <ul style="list-style-type: none">• TTI ACL 表示用于接口的 ACL 资源，当前设备仅用于 QinQ 和 VLAN 映射• PCL ACL 表示用于策略的 ACL 资源，包括协议报文使用 ACL 以及应用模块引用 ACL 时占用的资源• PCL Counter 表示用于策略的统计资源• IPCL Meter 表示用于入方向策略的流量监管资源• EPCL Meter 表示用于出方向策略的流量监管资源
Total	资源总数
Reserved	预留的资源数
Configured	已经使用的资源数
Remaining	剩余可用的资源数
Usage	预留的资源数与已配置的资源数之和占资源总数的百分比，分子按实际计算结果的整数部分显示，例如实际计算结果为50.8%，此处显示为50%。

1.1.12 packet-filter

packet-filter 命令用来在接口上应用 ACL 进行报文过滤。

undo packet-filter 命令用来取消在接口上应用 ACL 进行报文过滤。

【命令】

```
packet-filter [ ipv6 | mac ] { acl-number | name acl-name } { inbound | outbound }  
[ hardware-count ]  
undo packet-filter [ ipv6 | mac ] { acl-number | name acl-name } { inbound |  
outbound }
```

【缺省情况】

接口不对报文进行过滤。

【视图】

二层以太网接口视图/VLAN 接口视图

【缺省用户角色】

network-admin

【参数】

ipv6: 指定 ACL 类型为 IPv6 ACL。

mac: 指定 ACL 类型为二层 ACL。

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

- 2000~2999: 表示基本 ACL。
- 3000~3999: 表示高级 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。

inbound: 对收到的报文进行过滤。

outbound: 对发出的报文进行过滤。

hardware-count: 表示开启规则匹配硬件统计功能, 缺省为关闭。

【使用指导】

若未指定 **ipv6**、**mac** 关键字, 则表示 IPv4 ACL。

本命令中的 **hardware-count** 关键字用于开启指定 ACL 内所有规则的规则匹配硬件统计功能, 而 **rule** 命令中的 **counting** 关键字则用于开启当前规则的匹配统计功能。

如果设备资源不足, 必须先执行 **undo packet-filter** 命令取消报文过滤, 然后再配置不携带 **hardware-count** 关键字的报文过滤, 以此关闭规则匹配硬件统计功能。

如果设备资源充足, 可通过不携带 **hardware-count** 关键字重新配置报文过滤, 以此关闭规则匹配硬件统计功能。

一个接口在一个方向上最多可应用 3 个 ACL 进行报文过滤, 包括一个 IPv4 ACL (IPv4 基本 ACL 或 IPv4 高级 ACL)、一个 IPv6 ACL (IPv6 基本 ACL 或 IPv6 高级 ACL) 和一个二层 ACL。

VLAN 接口视图下配置的入方向报文过滤对所有报文生效, 包括通过 VLAN 接口进行三层转发的报文和通过 VLAN 接口对应的物理接口进行二层转发的报文。

VLAN 接口视图下配置的出方向报文过滤仅对通过 VLAN 接口进行三层转发的报文生效。

【举例】

应用 IPv4 基本 ACL 2001 对接口 GigabitEthernet1/0/1 收到的报文进行过滤，并开启规则匹配硬件统计功能。

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

【相关命令】

- **display packet-filter**
- **display packet-filter statistics**
- **display packet-filter verbose**

1.1.13 packet-filter default deny

packet-filter default deny 命令用来配置报文过滤的缺省动作为 Deny，即禁止未匹配上 ACL 规则的报文通过。

undo packet-filter default deny 命令用来恢复缺省情况。

【命令】

```
packet-filter default deny
undo packet-filter default deny
```

【缺省情况】

报文过滤的缺省动作为 Permit，即允许未匹配上 ACL 规则的报文通过。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

配置报文过滤的缺省动作会在所有的应用对象下添加一个缺省动作应用，该应用也会像其它应用的 ACL 一样显示。

【举例】

配置报文过滤的缺省动作为 Deny。

```
<Sysname> system-view
[Sysname] packet-filter default deny
```

【相关命令】

- **display packet-filter**
- **display packet-filter statistics**
- **display packet-filter verbose**

1.1.14 reset packet-filter statistics

reset packet-filter statistics 命令用来清除 ACL 在报文过滤中应用的统计信息。

【命令】

```
reset packet-filter statistics interface [ interface-type interface-number ]  
[ inbound | outbound ] [ [ ipv6 | mac ] { acl-number | name acl-name } ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface [*interface-type interface-number*]：清除指定接口上的统计信息。
interface-type interface-number 表示接口类型和接口编号。若未指定接口类型和接口编号，将清除所有接口上的统计信息。

inbound：清除入方向上的统计信息。

outbound：清除出方向上的统计信息。

ipv6：指定 ACL 类型为 IPv6 ACL。

mac：指定 ACL 类型为二层 ACL。

acl-number：清除指定编号 ACL 在报文过滤中应用的统计信息。*acl-number* 表示 ACL 的编号，取值范围及其代表的 ACL 类型如下：

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

name *acl-name*：清除指定名称 ACL 在报文过滤中应用的统计信息。*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

如果未指定 *acl-number*、**name** *acl-name* 和 ACL 类型（**ipv6**、**mac** 参数，将清除全部 ACL 在报文过滤中应用的统计信息。

如果未指定 **ipv6**、**mac** 参数，则表示 IPv4 ACL。

【举例】

清除在接口 GigabitEthernet1/0/1 入方向上 IPv4 基本 ACL 2001 在报文过滤中应用的统计信息。

```
<Sysname> reset packet-filter statistics interface gigabitethernet 1/0/1 inbound 2001
```

【相关命令】

- **display packet-filter statistics**
- **display packet-filter statistics sum**

1.1.15 rule (IPv4 advanced ACL view)

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。

【命令】

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

【缺省情况】

IPv4 高级 ACL 内不存在任何规则。

【视图】

IPv4 高级 ACL 视图

【缺省用户角色】

network-admin

【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，系统将从规则编号的起始值开始，自动分配一个大于现有最大编号的步长最小倍数。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 **icmp** (1)、**igmp** (2)、**ip**、**ipinip** (4)、**ospf** (89)、**tcp** (6) 或 **udp** (17)。**ip** 表示所有协议类型。

protocol之后可配置如 [表 1-7](#) 所示的规则信息参数。

表1-7 规则信息参数

参数	类别	作用	说明
source { <i>source-address</i> <i>source-wildcard</i> any }	源地址信息	指定ACL规则的源地址信息	<i>source-address</i> : 源IP地址 <i>source-wildcard</i> : 源IP地址的通配符掩码（为0表示主机地址） any : 任意源IP地址
destination { <i>dest-address</i> <i>dest-wildcard</i> any }	目的地址信息	指定ACL规则的目的地址信息	<i>dest-address</i> : 目的IP地址 <i>dest-wildcard</i> : 目的IP地址的通配符掩码（为0表示主机地址） any : 任意目的IP地址
counting	统计	开启规则匹配软件统计功能，缺省为关闭	本参数用于开启本规则的匹配统计功能，而 packet-filter 命令中的 hardware-count 关键字则用于开启指定ACL内所有规则的规则匹配硬件统计功能
precedence <i>precedence</i>	报文优先级	指定IP优先级	<i>precedence</i> 用数字表示时，取值范围为0~7；用字符表示时，分别对应 routine 、 priority 、 immediate 、 flash 、 flash-override 、 critical 、 internet 、 network
tos <i>tos</i>	报文优先级	指定ToS优先级	<i>tos</i> 用数字表示时，取值范围为0~15；用字符表示时，可以选取 max-reliability （2）、 max-throughput （4）、 min-delay （8）、 min-monetary-cost （1）、 normal （0）
dscp <i>dscp</i>	报文优先级	指定DSCP优先级	<i>dscp</i> 用数字表示时，取值范围为0~63；用字符表示时，可以选取 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）、 ef （46）
fragment	分片信息	仅对分片报文有效，而对非分片报文无效	若未指定该参数，则表示该规则对所有报文（包括非分片报文和分片报文的每个分片）均有效
logging	日志操作	对符合条件的报文可记录日志信息	该功能需要使用该ACL的模块支持日志记录功能，例如报文过滤
time-range <i>time-range-name</i>	时间段	指定本规则生效的时间段	<i>time-range-name</i> : 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。有关时间段的详细介绍和具体配置过程，请参见“ACL和QoS配置指导”中的“时间段”

当 *protocol* 为 **tcp**（6）或 **udp**（17）时，用户还可配置如 [表 1-8](#) 所示的规则信息参数。

表1-8 TCP/UDP 特有的规则信息参数

参数	类别	作用	说明
source-port <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> 为操作符，取值可以为 lt （小于）、 gt （大于）、 eq （等于）或者 range （在范围内，包括边界值）。只有操作符 range 需要两个端口号做操作数，其它的只需要一个端口号做操作数
destination-port <i>operator port1</i> [<i>port2</i>]	目的端口	定义TCP/UDP报文的端口信息	<i>port1</i> 、 <i>port2</i> : TCP或UDP的端口号，用数字表示时，取值范围为0~65535；用字符表示时，TCP端口号可以选取 chargen （19）、 cmd （514）、 daytime （13）、 discard （9）、 dns （53）、 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）、 www （80）；UDP端口号可以选取 biff （512）、 bootpc （68）、 bootps （67）、 discard （9）、 dns （53）、 dnsix （90）、 echo （7）、 mobilitip-ag （434）、 mobilitip-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）、 xmcp （177）
{ ack <i>ack-value</i> fin <i>fin-value</i> psh <i>psh-value</i> rst <i>rst-value</i> syn <i>syn-value</i> urg <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”。譬如：当配置为 ack 0 psh 1 时，表示匹配不携带ACK且携带PSH标志位的TCP报文
established	TCP连接建立标识	定义对TCP连接报文的处理规则	TCP协议特有的参数。 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 1-9](#) 所示的规则信息参数。

表1-9 ICMP 特有的规则信息参数

参数	类别	作用	说明
icmp-type { <i>icmp-type</i> <i>icmp-code</i> <i>icmp-message</i> }	ICMP报文的 消息类型和 消息码信息	指定本规则中 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。可以输入的ICMP消息名称，及其与消息类型和消息码的对应关系如 表 1-10 所示

表1-10 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

【使用指导】

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。

display acl all 命令可以查看所有已存在的 IPv4 高级 ACL 规则和 IPv4 基本 ACL 规则。

删除规则时需要注意的是：

- 使用 **undo rule rule-id** 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。
- **undo rule { deny | permit }** 命令无法删除规则中的部分内容，使用 **undo rule { deny | permit }** 命令时，必须输入已存在规则的完整形式。

【举例】

为 IPv4 高级 ACL 3000 创建规则如下：允许 129.9.0.0/16 网段内的主机与 202.38.160.0/24 网段内主机的 WWW 端口（端口号为 80）建立连接。

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule permit tcp source 129.9.0.0 0.0.255.255 destination
202.38.160.0 0.0.0.255 destination-port eq 80
```

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

```
<Sysname> system-view
[Sysname] acl advanced 3001
[Sysname-acl-ipv4-adv-3001] rule deny icmp destination 192.168.1.0 0.0.0.255
[Sysname-acl-ipv4-adv-3001] rule permit ip
```

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 advanced 3002
[Sysname-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp
[Sysname-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp-data
[Sysname-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp
[Sysname-acl-ipv4-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 advanced 3003
[Sysname-acl-ipv4-adv-3003] rule permit udp source-port eq snmp
[Sysname-acl-ipv4-adv-3003] rule permit udp source-port eq snmptrap
[Sysname-acl-ipv4-adv-3003] rule permit udp destination-port eq snmp
[Sysname-acl-ipv4-adv-3003] rule permit udp destination-port eq snmptrap
```

【相关命令】

- **acl**
- **acl logging interval**
- **display acl**
- **step**
- **time-range**（ACL 和 QoS 命令参考/时间段）

1.1.16 rule (IPv4 basic ACL view)

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。

【命令】

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

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

【缺省情况】

IPv4 基本 ACL 内不存在任何规则。

【视图】

IPv4 基本 ACL 视图

【缺省用户角色】

network-admin

【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，系统将从规则编号的起始值开始，自动分配一个大于现有最大编号的步长最小倍数。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: 表示开启规则匹配软件统计功能，缺省为关闭。

fragment: 表示仅对分片报文有效，而对非分片报文无效。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 {source-address source-wildcard | any }: 指定规则的源 IP 地址信息。
source-address 表示报文的源 IP 地址，*source-wildcard* 表示源 IP 地址的通配符掩码（为 0 表示主机地址），**any** 表示任意源 IP 地址。

time-range time-range-name: 指定本规则生效的时间段。*time-range-name* 表示时间段的名称，为 1~32 个字符的字符串，不区分大小写，必须以英文字母 a~z 或 A~Z 开头。若该时间段尚未配置，该规则仍会成功创建但系统将给出提示信息，并在该时间段的配置完成后此规则才会生效。有关时间段的详细介绍和具体配置过程，请参见“ACL 和 QoS 配置指导”中的“时间段”。

【使用指导】

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。

display acl all 命令可以查看所有已存在的 IPv4 高级 ACL 规则和 IPv4 基本 ACL 规则。

删除规则时需要注意的是：

- 使用 **undo rule rule-id** 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。
- **undo rule { deny | permit }** 命令无法删除规则中的部分内容，使用 **undo rule { deny | permit }** 命令时，必须输入已存在规则的完整形式。

counting 关键字用于开启本规则的匹配统计功能，而 **packet-filter** 命令中的 **hardware-count** 关键字则用于开启指定 ACL 内所有规则的规则匹配硬件统计功能。

【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 basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 10.0.0.0 0.255.255.255
[Sysname-acl-ipv4-basic-2000] rule permit source 172.17.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] rule deny source any
```

【相关命令】

- **acl**
- **acl logging interval**
- **display acl**
- **step**
- **time-range** (ACL 和 QoS 命令参考/时间段)

1.1.17 rule (IPv6 advanced ACL view)

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。

【命令】

```
rule [ rule-id ] { deny | permit } protocol [ { { ack ack-value | fin fin-value | psh psh-value | rst rst-value | syn syn-value | urg urg-value } * | established } |
counting | destination { dest-address dest-prefix | dest-address/dest-prefix | any } | destination-port operator port1 [ port2 ] |
dscp dscp | flow-label flow-label-value | fragment | icmp6-type { icmp6-type icmp6-code | icmp6-message } | logging | routing [ type routing-type ] |
hop-by-hop [ type hop-type ] | source { source-address source-prefix | source-address/source-prefix | any } | source-port operator port1 [ port2 ] |
time-range time-range-name ] *

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

undo rule { deny | permit } protocol [ { { ack ack-value | fin fin-value | psh psh-value | rst rst-value | syn syn-value | urg urg-value } * | established } |
counting | destination { dest-address dest-prefix | dest-address/dest-prefix | any } | destination-port operator port1 [ port2 ] |
dscp dscp | flow-label flow-label-value | fragment | icmp6-type { icmp6-type icmp6-code | icmp6-message } | logging | routing [ type routing-type ] |
```



```
hop-by-hop [ type hop-type ] | source { source-address source-prefix |
source-address/source-prefix | any } | source-port operator port1 [ port2 ] |
time-range time-range-name ] *
```

【缺省情况】

IPv6 高级 ACL 内不存在任何规则。

【视图】

IPv6 高级 ACL 视图

【缺省用户角色】

network-admin

【参数】

rule-id: 指定 IPv6 高级 ACL 规则的编号，取值范围为 0～65534。若未指定本参数，系统将从规则编号的起始值开始，自动分配一个大于现有最大编号的步长最小倍数。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 **icmpv6**（58）、**ipv6**、**ipv6-ah**（51）、**ipv6-esp**（50）、**ospf**（89）、**tcp**（6）或 **udp**（17）。**ipv6** 表示所有协议类型。

protocol之后可配置如 [表 1-11](#)所示的规则信息参数。

表1-11 规则信息参数

参数	类别	作用	说明
source { <i>source-address</i> <i>source-prefix</i> <i>source-address/source-prefix</i> any }	源IPv6地址	指定ACL规则的源IPv6地址信息	<i>source-address</i> : 源IPv6地址 <i>source-prefix</i> : 源IPv6地址的前缀长度，取值范围1～128 any : 任意源IPv6地址
destination { <i>dest-address</i> <i>dest-prefix</i> <i>dest-address/dest-prefix</i> any }	目的IPv6地址	指定ACL规则的目的地IPv6地址信息	<i>dest-address</i> : 目的IPv6地址 <i>dest-prefix</i> : 目的IPv6地址的前缀长度，取值范围1～128 any : 任意目的IPv6地址
counting	统计	开启规则匹配软件统计功能，缺省为关闭	本参数用于开启本规则的匹配统计功能，而 packet-filter ipv6 命令中的 hardware-count 关键字则用于开启指定ACL内所有规则的规则匹配硬件统计功能

参数	类别	作用	说明
dscp <i>dscp</i>	报文优先级	指定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 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 <i>flow-label-value</i>	流标签字段	指定IPv6基本报文头中流标签字段的值	<i>flow-label-value</i> : 流标签字段的值, 取值范围为0~1048575
fragment	报文分片	仅对分片报文有效, 而对非分片报文无效	若未指定本参数, 表示该规则对所有报文 (包括非分片报文和分片报文的每个分片) 均有效
logging	日志操作	对符合条件的报文可记录日志信息	该功能需要使用该ACL的模块支持日志记录功能, 例如报文过滤
routing [type <i>routing-type</i>]	路由头	指定路由头的类型	<i>routing-type</i> : 路由头类型的值, 取值范围为0~255 若指定了 type <i>routing-type</i> 参数, 表示仅对指定类型的路由头有效; 否则, 表示对IPv6所有类型的路由头都有效
hop-by-hop [type <i>hop-type</i>]	逐跳头	指定逐跳头的类型	<i>hop-type</i> : 逐跳头类型的值, 取值范围为0~255 若指定了 type <i>hop-type</i> 参数, 表示仅对指定类型的逐跳头有效; 否则, 表示对IPv6所有类型的逐跳头都有效
time-range <i>time-range-name</i>	时间段	指定本规则生效的时间段	<i>time-range-name</i> : 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。有关时间段的详细介绍和具体配置过程, 请参见“ACL和QoS配置指导”中的“时间段”

当`protocol`为**tcp** (6) 或**udp** (17) 时, 用户还可配置如 [表 1-12](#) 所示的规则信息参数。

表1-12 TCP/UDP 特有的规则信息参数

参数	类别	作用	说明
source-port <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 lt (小于)、 gt (大于)、 eq (等于) 或者 range (在范围内, 包括边界值)。只有 range 操作符需要两个端口号做操作数, 其它操作符只需要一个端口号做操作数
destination-port <i>operator port1</i> [<i>port2</i>]	目的端口	定义TCP/UDP报文的端口信息	<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 chargen (19)、 cmd (514)、 daytime (13)、 discard (9)、 dns (53)、 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)、 mobilitip-ag (434)、 mobilitip-mn (435)、 nameserver (42)、 netbios-dgm (138)、 netbios-ns (137)、 netbios-ssn (139)、 ntp (123)、 rip (520)、 snmp (161)、 snmptrap (162)、 sunrpc (111)、 syslog (514)、 tacacs-ds (65)、 talk (517)、 tftp (69)、 time (37)、 who (513) 或 xdmcp (177)
{ ack <i>ack-value</i> fin <i>fin-value</i> psh <i>psh-value</i> rst <i>rst-value</i> syn <i>syn-value</i> urg <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) 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”。譬如: 当配置为 ack 0 psh 1 时, 表示匹配不携带ACK且携带PSH标志位的TCP报文
established	TCP连接建立标识	定义对TCP连接报文的处理规则	TCP协议特有的参数。 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 1-13](#) 所示的规则信息参数。

表1-13 ICMPv6 特有的规则信息参数

参数	类别	作用	说明
icmp6-type { <i>icmp6-type</i> <i>icmp6-code</i> <i>icmp6-message</i> }	ICMPv6报文的 消息类型和 消息码	指定本规则中 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 表1-14 所示

表1-14 ICMPv6 消息名称与消息类型和消息码的对应关系

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

【使用指导】

- 当 ACL 用于 QoS 策略的流分类或报文过滤功能时：
- 规则不支持配置 **fragment** 参数。
- 如果 QoS 策略或报文过滤功能应用于出方向，规则不支持配置 **routing**、**hop-by-hop**、**flow-label** 参数。

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。

display acl ipv6 all 命令可以查看所有已存在的 IPv6 高级 ACL 规则和 IPv6 基本 ACL 规则。

删除规则时需要注意的是：

- 使用 **undo rule rule-id** 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。
- **undo rule { deny | permit }** 命令无法删除规则中的部分内容，使用 **undo rule { deny | permit }** 命令时，必须输入已存在规则的完整形式。

【举例】

为 IPv6 高级 ACL 3000 创建规则如下：允许 2030:5060::/64 网段内的主机与 FE80:5060::/96 网段内主机的 WWW 端口（端口号为 80）建立连接。

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

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 advanced 3001
[Sysname-acl-ipv6-adv-3001] rule deny icmpv6 destination fe80:5060:1001:: 48
[Sysname-acl-ipv6-adv-3001] rule permit ipv6
```

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 advanced 3002
[Sysname-acl-ipv6-adv-3002] rule permit tcp source-port eq ftp
[Sysname-acl-ipv6-adv-3002] rule permit tcp source-port eq ftp-data
[Sysname-acl-ipv6-adv-3002] rule permit tcp destination-port eq ftp
[Sysname-acl-ipv6-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 advanced 3003
[Sysname-acl-ipv6-adv-3003] rule permit udp source-port eq snmp
[Sysname-acl-ipv6-adv-3003] rule permit udp source-port eq snmptrap
[Sysname-acl-ipv6-adv-3003] rule permit udp destination-port eq snmp
[Sysname-acl-ipv6-adv-3003] rule permit udp destination-port eq snmptrap
```

为 IPv6 高级 ACL 3004 创建规则如下：在含有逐跳头的报文中，只允许转发含有 MLD 选项（Type =5）的报文，丢弃其他报文。

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3004
[Sysname-acl-ipv6-adv-3004] rule permit ipv6 hop-by-hop type 5
[Sysname-acl-ipv6-adv-3004] rule deny ipv6 hop-by-hop
```

【相关命令】

- **acl**
- **acl logging interval**
- **display acl**
- **step**
- **time-range**（ACL 和 QoS 命令参考/时间段）

1.1.18 rule (IPv6 basic ACL view)

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。

【命令】

```
rule [ rule-id ] { deny | permit } [ counting | fragment | logging | routing  
[ type routing-type ] | source { source-address source-prefix |  
source-address/source-prefix | any } | time-range time-range-name ] *  
undo rule rule-id [ counting | fragment | logging | routing | source |  
time-range ] *  
undo rule { deny | permit } [ counting | fragment | logging | routing [ type  
routing-type ] | source { source-address source-prefix |  
source-address/source-prefix | any } | time-range time-range-name ] *
```

【缺省情况】

IPv6 基本 ACL 内不存在任何规则。

【视图】

IPv6 基本 ACL 视图

【缺省用户角色】

network-admin

【参数】

rule-id: 指定 IPv6 基本 ACL 规则的编号, 取值范围为 0~65534。若未指定本参数, 系统将从规则编号的起始值开始, 自动分配一个大于现有最大编号的步长最小倍数。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: 表示开启规则匹配软件统计功能, 缺省为关闭。

fragment: 表示仅对分片报文有效, 而对非分片报文无效。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 IPv6 所有类型的路由头都有效。

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

time-range time-range-name: 指定本规则生效的时间段。*time-range-name* 表示时间段的名称, 为 1~32 个字符的字符串, 不区分大小写, 必须以英文字母 a~z 或 A~Z 开头。若该时间段尚未配置, 该规则仍会成功创建但系统将给出提示信息, 并在该时间段的配置完成后此规则才会生效。有关时间段的详细介绍和具体配置过程, 请参见“ACL 和 QoS 配置指导”中的“时间段”。

【使用指导】

当 ACL 用于 QoS 策略的流分类或用于报文过滤功能时：

- 规则不支持配置 **fragment** 参数。
- 若 QoS 策略或报文过滤功能应用于出方向，规则不支持配置 **routing** 参数。

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。

display acl ipv6 all 命令可以查看所有已存在的 IPv6 高级 ACL 规则和 IPv6 基本 ACL 规则。

删除规则时需要注意的是：

- 使用 **undo rule rule-id** 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。
- **undo rule { deny | permit }** 命令无法删除规则中的部分内容，使用 **undo rule { deny | permit }** 命令时，必须输入已存在规则的完整形式。

counting 关键字用于开启本规则的匹配统计功能，而 **packet-filter ipv6** 命令中的 **hardware-count** 关键字则用于开启指定 ACL 内所有规则的规则匹配硬件统计功能。

【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 basic 2000
[Sysname-acl-ipv6-basic-2000] rule permit source 1001:: 16
[Sysname-acl-ipv6-basic-2000] rule permit source 3124:1123:: 32
[Sysname-acl-ipv6-basic-2000] rule permit source fe80:5060:1001:: 48
[Sysname-acl-ipv6-basic-2000] rule deny source any
```

【相关命令】

- **acl**
- **acl logging interval**
- **display acl**
- **step**
- **time-range** (ACL 和 QoS 命令参考/时间段)

1.1.19 rule (Layer 2 ACL view)

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。

【命令】

```
rule [ rule-id ] { deny | permit } [ cos dot1p | counting | dest-mac dest-address
dest-mask | { lsap lsap-type lsap-type-mask | type protocol-type
```



```

protocol-type-mask } | source-mac source-address source-mask | time-range
time-range-name ] *
undo rule rule-id [ counting | time-range ] *
undo rule { deny | permit } [ cos dot1p | counting | dest-mac dest-address
dest-mask | { lsap lsap-type lsap-type-mask | type protocol-type
protocol-type-mask } | source-mac source-address source-mask | time-range
time-range-name ] *

```

【缺省情况】

二层 ACL 内不存在任何规则。

【视图】

二层 ACL 视图

【缺省用户角色】

network-admin

【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, 系统将从规则编号的起始值开始, 自动分配一个大于现有最大编号的步长最小倍数。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 dot1p: 指定 802.1p 优先级。dot1p 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: 表示开启规则匹配软件统计功能, 缺省为关闭。

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

lsap lsap-type lsap-type-mask: 指定 LLC 封装中的 DSAP 字段和 SSAP 字段。lsap-type 表示数据帧的封装格式, 取值范围为十六进制数 0~ffff。lsap-type-mask 表示 LSAP 的类型掩码, 用于指定屏蔽位, 取值范围为十六进制数 0~ffff。

type protocol-type protocol-type-mask: 指定链路层协议类型。protocol-type 表示数据帧类型, 对应 Ethernet_II 类型和 Ethernet_SNAP 类型帧中的 type 域, 取值范围为十六进制数 0~ffff。protocol-type-mask 表示类型掩码, 用于指定屏蔽位, 取值范围为十六进制数 0~ffff。

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

time-range time-range-name: 指定本规则生效的时间段。time-range-name 表示时间段的名称, 为 1~32 个字符的字符串, 不区分大小写, 必须以英文字母 a~z 或 A~Z 开头。若该时间段尚未配置, 该规则仍会成功创建但系统将给出提示信息, 并在该时间段的配置完成后此规则才会生效。有关时间段的详细介绍和具体配置过程, 请参见“ACL 和 QoS 配置指导”中的“时间段”。

【使用指导】

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。

display acl mac all 命令可以查看所有已存在的二层 ACL 规则。

删除规则时需要注意的是：

- 使用 **undo rule rule-id** 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。
- **undo rule { deny | permit }** 命令无法删除规则中的部分内容，使用 **undo rule { deny | permit }** 命令时，必须输入已存在规则的完整形式。

counting 关键字用于开启本规则的匹配统计功能，而 **packet-filter** 命令中的 **hardware-count** 关键字则用于开启指定 ACL 内所有规则的规则匹配硬件统计功能。

【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 mac 4000
[Sysname-acl-mac-4000] rule permit type 0806 ffff
[Sysname-acl-mac-4000] rule deny type 8035 ffff
```

【相关命令】

- **acl**
- **display acl**
- **step**
- **time-range**（ACL 和 QoS 命令参考/时间段）

1.1.20 rule comment

rule comment 命令用来为规则配置描述信息。

undo rule comment 命令用来删除指定规则的描述信息。

【命令】

```
rule rule-id comment text
undo rule rule-id comment
```

【缺省情况】

规则没有描述信息。

【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

【缺省用户角色】

network-admin

【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。

【使用指导】

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。

【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 basic 2000
```

```
[Sysname-acl-ipv4-basic-2000] rule 0 deny source 1.1.1.1 0
```

```
[Sysname-acl-ipv4-basic-2000] rule 0 comment This rule is used on gigabitethernet 1/0/1.
```

【相关命令】

- **display acl**

1.1.21 step

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。

【命令】

```
step step-value [ start start-value ]
```

```
undo step
```

【缺省情况】

规则编号的步长为 5，起始值为 0。

【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

【缺省用户角色】

network-admin

【参数】

step-value: 表示规则编号的步长值，取值范围为 1～20。

start-value: 表示规则编号的起始值。取值范围为 0～20。

【使用指导】

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

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

【举例】

将 IPv4 基本 ACL 2000 的规则编号的步长配置为 2。

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] step 2
```

【相关命令】

- **display acl**

目 录

1 QoS策略.....	1-1
1.1 定义类的命令.....	1-1
1.1.1 description	1-1
1.1.2 display traffic classifier	1-1
1.1.3 if-match	1-2
1.1.4 traffic classifier	1-5
1.2 定义流行为的命令.....	1-6
1.2.1 accounting	1-6
1.2.2 car.....	1-6
1.2.3 display traffic behavior	1-8
1.2.4 filter	1-9
1.2.5 nest top-most.....	1-10
1.2.6 redirect.....	1-10
1.2.7 remark dot1p	1-11
1.2.8 remark dscp	1-12
1.2.9 remark local-precedence	1-14
1.2.10 remark service-vlan-id.....	1-14
1.2.11 traffic behavior.....	1-15
1.3 定义和应用QoS策略的命令.....	1-15
1.3.1 classifier behavior.....	1-15
1.3.2 display qos policy	1-16
1.3.3 display qos policy global.....	1-18
1.3.4 display qos policy interface	1-19
1.3.5 display qos policy user-profile.....	1-22
1.3.6 display qos vlan-policy	1-24
1.3.7 qos apply policy (interface view).....	1-25
1.3.8 qos apply policy (user profile view)	1-26
1.3.9 qos apply policy global.....	1-26
1.3.10 qos policy.....	1-27
1.3.11 qos vlan-policy	1-28
1.3.12 reset qos policy global.....	1-28
1.3.13 reset qos vlan-policy.....	1-29

2 优先级映射	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	2-2
2.2 端口优先级信任模式配置命令	2-3
2.2.1 display qos trust interface	2-3
2.2.2 qos trust	2-4
2.3 端口优先级配置命令	2-5
2.3.1 qos priority	2-5
3 流量整形和限速	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	3-1
3.2 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	4-5
4.1 拥塞管理公共配置命令	4-5
4.1.1 display qos queue interface	4-5
4.2 严格优先级队列配置命令	4-6
4.2.1 display qos queue sp interface	4-6
4.2.2 qos sp	4-6
4.3 加权轮询队列配置命令	4-7
4.3.1 display qos queue wrr interface	4-7
4.3.2 qos wrr	4-8
4.3.3 qos wrr weight	4-9
4.3.4 qos wrr group sp	4-10
4.4 队列调度策略配置命令	4-11
4.4.1 display qos qmprofile configuration	4-11
4.4.2 display qos qmprofile interface	4-12
4.4.3 qos apply qmprofile	4-12
4.4.4 qos qmprofile	4-13
4.4.5 queue	4-14
4.5 端口队列统计配置命令	4-15
4.5.1 display qos queue-statistics interface outbound	4-15

5 聚合CAR	5-1
5.1 聚合CAR配置命令	5-1
5.1.1 car name	5-1
5.1.2 display qos car name.....	5-1
5.1.3 qos car	5-3
5.1.4 reset qos car name	5-4

1 QoS策略

1.1 定义类的命令

1.1.1 description

description 命令用来配置类的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

```
description text
undo description
```

【缺省情况】

未配置类的描述信息。

【视图】

类视图

【缺省用户角色】

network-admin

【参数】

text: 表示类的描述信息，为 1~127 个字符的字符串，区分大小写。

【使用指导】

多次执行本命令，最后一次执行的命令生效。

【举例】

```
# 为类 class1 配置描述信息。
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] description classifier
```

1.1.2 display traffic classifier

display traffic classifier 命令用来显示类的配置信息。

【命令】

```
display traffic classifier user-defined [ classifier-name ] [ slot
slot-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

user-defined: 用户定义类。

classifier-name: 类名，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，将显示所有类的配置信息。

slot slot-number: 显示指定成员设备的流分类的信息，*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，将显示主用设备的类的配置信息。

【举例】

```
# 显示用户定义类的配置信息。
<Sysname> display traffic classifier user-defined

User-defined classifier information:

Classifier: 1 (ID 100)
  Operator: AND
  Rule(s) :
    If-match acl 2000

Classifier: 2 (ID 101)
  Operator: AND
  Rule(s) :
    If-match protocol ipv6

Classifier: 3 (ID 102)
  Operator: AND
  Rule(s) :
    -none-
```

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

1.1.3 if-match

if-match 命令用来定义匹配数据包的规则。

undo if-match 命令用来删除配置的匹配数据包的规则。

【命令】

```
if-match match-criteria
```


undo if-match match-criteria

【缺省情况】

未定义匹配数据包的规则。

【视图】

类视图

【缺省用户角色】

network-admin

【参数】

match-criteria: 类的匹配规则，具体情况如 [表 1-2](#) 所示。

表1-2 类的匹配规则取值

取值	描述
acl [ipv6 mac] { acl-number name acl-name }	定义匹配ACL的规则 acl-number 是ACL的序号，IPv4 ACL序号的取值范围是2000～3999，IPv6 ACL序号的取值范围是2000～3999，二层ACL序号的取值范围是4000～4999 acl-name 是ACL的名称，为1～63个字符的字符串，不区分大小写，必须以英文字母a～z或A～Z开头，为避免混淆，ACL的名称不可以使用英文单词all
any	定义匹配所有数据包的规则
destination-mac mac-address	定义匹配目的MAC地址的规则，仅对以太网接口生效
dscp dscp-value&<1-8>	定义匹配DSCP的规则， dscp-value&<1-8> 为DSCP取值的列表，DSCP的取值范围为0～63，&<1-8>表示前面的参数最多可以输入8次；也可以输入关键字，具体如 表1-4 所示
protocol protocol-name	定义匹配协议的规则， protocol-name 取值为ip、ipv6
service-dot1p dot1p-value&<1-8>	定义匹配外层VLAN Tag 802.1p优先级的规则， dot1p-value&<1-8> 为802.1p优先级值的列表，802.1p优先级的取值范围为0～7，&<1-8>表示前面的参数最多可以输入8次
service-vlan-id vlan-id-list	定义匹配外层VLAN Tag VLAN ID的规则， vlan-id-list : VLAN列表，表示方式为 vlan-id-list = { vlan-id vlan-id1 to vlan-id2 }&<1-10> ， vlan-id 、 vlan-id1 、 vlan-id2 取值范围为1～4094，且 vlan-id1 的值必须小于 vlan-id2 的值；&<1-10>表示前面的参数最多可以重复输入10次 若只携带单层VLAN Tag，可以用外层VLAN Tag的VLAN ID规则来匹配
source-mac mac-address	定义匹配源MAC地址的规则，仅对以太网接口生效

【使用指导】

一个类下可配置多条匹配命令，各个配置之间互相不覆盖。

在定义匹配规则（DSCP、VLAN ID 和 802.1p 优先级）时，请注意：

- 一条命令可以配置多个规则，如果指定了多个相同的规则，系统默认为一个；一条命令中多个不同的规则是或的关系，即只要有一个值匹配，就算匹配这条规则。
- 删除某条匹配的规则时，必须与该规则中定义的完全相同才会删除，顺序可以不同。

在定义匹配 ACL 的规则时，类中引用的 ACL 必须已经存在。

当 **if-match** 中引用的 ACL 规则的动作作为 **deny** 时，则直接忽略 ACL 规则的动作，以流行为中定义的动作为准，报文匹配只使用 ACL 中的分类域。

在定义匹配类的规则时，如果匹配类的规则之间既有逻辑与，又有逻辑或的关系，请使用以下方式配置。例如，需要定义 classA，满足以下关系：规则 1 & 规则 2 | 规则 3，可以这样定义：

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

【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：匹配外层 VLAN Tag 的 802.1p 优先级为 5。

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

定义类匹配 ACL3101。

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

定义类匹配 ACL flow。

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

定义类匹配 IPv6 ACL3101。

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

定义类匹配 IPv6 ACL flow。

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

定义匹配所有数据包的规则。

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

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

```

<Sysname> system-view
[Sysname] traffic classifier class1 operator or
[Sysname-classifier-class1] if-match dscp 1 6 9
# 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：匹配外层 VLAN Tag 的 VLAN ID 值为 2 或 7 或 10 的报文。

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

```

1.1.4 traffic classifier

traffic classifier 命令用来创建一个类，并进入类视图。如果指定的类已经存在，则直接进入类视图。

undo traffic classifier 命令用来删除一个类。

【命令】

```

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

```

【缺省情况】

未配置类。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

classifier-name: 类名，为 1~31 个字符的字符串，区分大小写。

operator: 指定各规则之间的逻辑运算符。缺省情况为 **and**。

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。

【举例】

定义一个名为 class1 的类。

```

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

```

【相关命令】

- **display traffic classifier**

1.2 定义流行为的命令

1.2.1 accounting

accounting 命令用来配置流量统计动作。

undo accounting 命令用来恢复缺省情况。

【命令】

```
accounting { byte | packet }  
undo accounting
```

【缺省情况】

未配置流量统计动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

byte: 表示报文基于字节进行统计。

packet: 表示报文基于包进行统计。

【举例】

为流行为配置流量统计动作，基于字节进行统计。

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

1.2.2 car

car 命令用来配置流量监管动作。

undo car 命令用来恢复缺省情况。

【命令】

```
car cir committed-information-rate [ cbs committed-burst-size [ ebs  
excess-burst-size ] ] [ green action | red action | yellow action ] *  
car cir committed-information-rate [ cbs committed-burst-size ] pir  
peak-information-rate [ ebs excess-burst-size ] [ green action | red action |  
yellow action ] *  
undo car
```

【缺省情况】

未配置流量监管动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【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 8~160000000 且必须为 8 的整数倍。

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

- 如果不指定 **cbs** 参数，缺省取值为与 $62.5 \times \text{committed-information-rate}$ 的乘积最接近且不小于 512 的整数倍，但是最大值不能超过 256000000。
- 如果指定 **cbs** 参数，取值范围 512~256000000 且必须为 512 的整数倍。

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

配置 **pir** 参数后：

- 如果不指定 **ebs**，则 **ebs** 缺省取值为与 $62.5 \times \text{peak-information-rate}$ 的乘积最接近且不小于 512 的整数倍，但是最大值不能超过 256000000。
- 如果指定 **ebs**，取值范围 0~256000000 且必须为 512 的整数倍。

未配置 **pir** 参数时，**ebs** 的取值范围为 0~256000000 且必须为 512 的整数倍。

pir *peak-information-rate*: 峰值速率，单位为 kbps，取值范围为 8~160000000 且必须为 8 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**。

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**。

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**。

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-dot1p-pass** *new-cos*: 设置新的 802.1P 报文的优先级值，并允许数据包通过，取值范围为 0~7。
- **remark-dscp-pass** *new-dscp*: 设置报文新的 DSCP 值，并允许数据包通过，取值范围为 0~63。
- **remark-lp-pass** *new-local-precedence*: 设置新的本地优先级，并允许数据包通过，取值范围为 0~7。

【使用指导】

在同一个流行为中多次执行本命令，最后一次执行的命令生效。

如果未配置峰值速率，则表示所配置的是单速率流量监管，否则表示双速率流量监管。

【举例】

为流行为配置流量监管。报文正常流速为 200kbps，承诺突发尺寸为 51200bytes，速率大于 200kbps 时，报文 DSCP 值改为 0 并发送。

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

```
[Sysname] traffic behavior database
```

```
[Sysname-behavior-database] car cir 200 cbs 51200 ebs 0 green pass red remark-dscp-pass 0
```

1.2.3 display traffic behavior

display traffic behavior 命令用来显示流行为的配置信息。

【命令】

```
display traffic behavior user-defined [ behavior-name ] [ slot slot-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【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，区分大小写。如果未指定本参数，则显示所有流行为的配置信息。

slot slot-number: 显示指定成员设备的流行为的信息，*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示主用设备的流行为的配置信息。

【举例】

显示用户定义行为的配置信息。

```
<Sysname> display traffic behavior user-defined
```

```
User-defined behavior information:
```

```
Behavior: 1 (ID 100)
  Marking:
    Remark dscp 3
  Committed Access Rate:
    CIR 112 (kbps), CBS 5120 (Bytes), EBS 512 (Bytes)
  Green action : pass
  Yellow action : pass
  Red action   : discard
```

```
Behavior: 2 (ID 101)
  Accounting enable: Packet
  Filter enable: Permit
  Redirecting:
    Redirect to the CPU
```

```
Behavior: 3 (ID 102)
  -none-
```

表1-3 display traffic behavior 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	标记相关信息
Remark dscp	重新标记报文的DSCP优先级值
Committed Access Rate	流量限速的相关信息
CIR	承诺信息速率，单位为kbps
CBS	承诺突发尺寸，单位为byte
EBS	超出突发尺寸，单位为byte
Green action	对绿色报文的动作
Red action	对红色报文的动作
Yellow action	对黄色报文的动作
Accounting enable	流量统计动作
Filter enable	流量过滤动作
Redirecting	流量重定向相关信息
Mirroring	流量镜像相关信息
none	表示未配置其他流行为

1.2.4 filter

filter 命令用来配置流量过滤动作。

undo filter 命令用来恢复缺省情况。

【命令】

```
filter { deny | permit }
undo filter
```

【缺省情况】

未配置流量过滤动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

deny: 丢弃数据包。

permit: 允许数据包通过。

【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 nest top-most

nest top-most 命令用来配置添加报文的外层 VLAN Tag 动作。

undo nest top-most 命令用来恢复缺省情况。

【命令】

```
nest top-most vlan vlan-id
undo nest top-most
```

【缺省情况】

未配置添加报文外层 VLAN Tag 动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

vlan vlan-id: 添加的 VLAN ID，取值范围为 1~4094。

【使用指导】

引用了添加 VLAN Tag 动作的 QoS 策略只能应用到接口的入方向上。

在同一个流行为中多次执行本命令，最后一次执行的命令生效。

【举例】

在流行为 b1 上配置如下动作：添加 VLAN ID 为 123 的外层 VLAN Tag。

```
<Sysname> system-view
[Sysname] traffic behavior b1
[Sysname-behavior-b1] nest top-most vlan 123
```

1.2.6 redirect

redirect 命令用来为流行为配置流量重定向动作。

undo redirect 命令用来恢复缺省情况。

【命令】

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


【缺省情况】

未配置流量重定向动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【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。

【使用指导】

在同一个流行为中多次执行本命令，最后一次执行的命令生效。

设备仅支持在入方向应用 QoS 策略配置流量重定向。

配置重定向到指定接口时，必须保证：

- 报文入接口的 VLAN ID 与指定接口的缺省 VLAN ID 相同；
- 报文入接口的 VLAN ID 在指定接口允许通过的 VLAN ID 列表中；

否则报文到达重定向到指定接口后会被丢弃。

基于上线用户应用 QoS 策略时，如果配置重定向到接口，则需确保 **redirect** 命令中指定的接口与重定向报文进入设备的接口属于同一 VLAN。

【举例】

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

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

【相关命令】

- **classifier behavior**
- **qos policy**
- **traffic behavior**

1.2.7 remark dot1p

remark dot1p 命令用来配置重新标记报文的 802.1p 优先级或内外层标签 802.1p 优先级复制动作。

undo remark dot1p 命令用来恢复缺省情况。

【命令】

```
remark [ green | red | yellow ] dot1p dot1p-value
undo remark [ green | red | yellow ] dot1p
remark dot1p customer-dot1p-trust
```

undo remark dot1p

【缺省情况】

未配置重新标记报文 802.1p 优先级以及内外层标签 802.1p 优先级复制动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

green: 对绿色报文进行重新标记。

red: 对红色报文进行重新标记。

yellow: 对黄色报文进行重新标记。

dot1p-value: 802.1p 优先级，取值范围为 0~7。

customer-dot1p-trust: 将内层 VLAN tag 的 802.1p 优先级复制为外层 VLAN tag 的 802.1p 优先级。

【使用指导】

命令 **remark dot1p dot1p-value** 和 **remark dot1p customer-dot1p-trust** 是覆盖关系。对于只携带一层 VLAN tag 的报文，配置的 **remark dot1p customer-dot1p-trust** 不会生效。在同一个流行为中，如果多次对同一种颜色的报文重新标记 802.1p 优先级，则最后一次执行的命令生效。

设备仅支持在入方向应用 QoS 策略配置重新标记报文的 802.1p 优先级。

【举例】

重新标记报文的 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
```

1.2.8 remark dscp

remark dscp 命令用来重新标记报文的 DSCP 值。

undo remark dscp 命令用来恢复缺省情况。

【命令】

remark [green | red | yellow] dscp dscp-value

undo remark [green | red | yellow] dscp

【缺省情况】

未配置重新标记报文 DSCP 值的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

green: 对绿色报文进行重新标记。

red: 对红色报文进行重新标记。

yellow: 对黄色报文进行重新标记。

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）
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
default	000000	0
ef	101110	46

【举例】

重新标记报文的 DSCP 值为 6。

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

```
[Sysname] traffic behavior database
[Sysname-behavior-database] remark dscp 6
```

1.2.9 remark local-precedence

remark local-precedence 命令用来重新标记报文的本地优先级。

undo remark local-precedence 命令用来恢复缺省情况。

【命令】

```
remark local-precedence local-precedence-value
undo remark local-precedence
```

【缺省情况】

未配置重新标记报文本地优先级的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

local-precedence-value: 本地优先级，取值范围为 0~7。

【使用指导】

设备仅支持在入方向应用 QoS 策略配置重新标记报文的本地优先级。

【举例】

```
# 重新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
```

1.2.10 remark service-vlan-id

remark service-vlan-id 命令用来重新标记报文的 SVLAN。

undo remark service-vlan-id 命令用来恢复缺省情况。

【命令】

```
remark service-vlan-id vlan-id
undo remark service-vlan-id
```

【缺省情况】

未配置重新标记报文的 SVLAN 的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

vlan-id: 表示重新标记报文外层 VLAN（SVLAN）的编号，取值范围为 1～4094。

【举例】

在流行为 b1 上配置重新标记报文的 SVLAN 为 VLAN 222。

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

1.2.11 traffic behavior

traffic behavior 命令用来创建一个流行为，并进入流行为视图。如果指定的流行为已经存在，则直接进入流行为视图。

undo traffic behavior 命令用来删除一个流行为。

【命令】

```
traffic behavior behavior-name
undo traffic behavior behavior-name
```

【缺省情况】

不存在流行为。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

behavior-name: 流行为名，为 1～31 个字符的字符串，区分大小写。

【举例】

定义一个名为 behavior1 的流行为。

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

【相关命令】

- **display traffic behavior**

1.3 定义和应用QoS策略的命令

1.3.1 classifier behavior

classifier behavior 命令用来为类指定流行为。

undo classifier 命令用来取消为类指定的流行为。

【命令】

```
classifier classifier-name behavior behavior-name [ insert-before
before-classifier-name ]
undo classifier classifier-name
```

【缺省情况】

没有为类指定流行为。

【视图】

QoS 策略视图

【缺省用户角色】

network-admin

【参数】

classifier-name: 类名，为 1~31 个字符的字符串，区分大小写。

behavior-name: 流行为名，为 1~31 个字符的字符串，区分大小写。

insert-before before-classifier-name: 表示将配置的类插入到 QoS 策略中已存在的指定类之前。**before-classifier-name** 表示 QoS 策略中已存在的类名，为 1~31 个字符的字符串，区分大小写。不指定该参数时，表示新配置的类与流行为配对将添加到 QoS 策略最后。

【使用指导】

QoS 策略下每个类只能与一个流行为关联。

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。

【举例】

在 QoS 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
```

在 QoS 策略 user1 中为类 database 指定流行为 test，并将该类插入到策略中已存在的类 class-a 前。

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

【相关命令】

- **qos policy**

1.3.2 display qos policy

display qos policy 命令用来显示 QoS 策略的配置信息。

【命令】

```
display qos policy user-defined [ policy-name [ classifier classifier-name ] ]
[ slot slot-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

user-defined: 用户定义 QoS 策略。

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

classifier classifier-name: QoS 策略中的类名，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则显示策略中所有类相关的配置信息。

slot slot-number: 显示指定成员设备的 QoS 策略的信息，*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示主用设备的 QoS 策略的配置信息。

【举例】

```
# 显示用户定义 QoS 策略的配置信息。
<Sysname> display qos policy user-defined

User-defined QoS policy information:

Policy: 1 (ID 100)
Classifier: 1 (ID 100)
Behavior: 1
Marking:
    Remark dscp 3
Committed Access Rate:
    CIR 112 (kbps), CBS 51200 (Bytes), EBS 512 (Bytes)
Green action : pass
Yellow action : pass
Red action   : discard
Classifier: 2 (ID 101)
Behavior: 2
Accounting enable: Packet
Filter enable: Permit
Marking:
    Remark dot1p 4
Classifier: 3 (ID 102)
Behavior: 3
-none-
```

表1-5 display qos policy 命令显示信息描述表

字段	描述
User-defined QoS policy information	用户自定义QoS策略的信息

其它显示信息解释请参见 [表 1-1](#) 和 [表 1-3](#)。

1.3.3 display qos policy global

display qos policy global 命令用来显示基于全局应用 QoS 策略的配置信息和运行情况。

【命令】

display qos policy global [*slot slot-number*] [*inbound* | *outbound*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

inbound: 显示入方向 QoS 策略的配置信息和运行情况。

outbound: 显示出方向 QoS 策略的配置信息和运行情况。

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* 表示设备在 IRF 中的成员编号。如果未指定本参数, 则显示主设备上基于全局应用 QoS 策略的信息。

【使用指导】

如果未指定显示方向, 则同时显示出入两个方向 QoS 策略的配置信息和运行情况。

【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: 1
Operator: AND
Rule(s) :
  If-match acl 2000
Behavior: 1
Marking:
  Remark dscp 3
Committed Access Rate:
  CIR 112 (kbps), CBS 51200 (Bytes), EBS 512 (Bytes)
  Green action : pass
  Yellow action : pass
  Red action   : discard
  Green packets : 0 (Packets) 0 (Bytes)
  Yellow packets: 0 (Packets) 0 (Bytes)
  Red packets   : 0 (Packets) 0 (Bytes)
Classifier: 2
Operator: AND
Rule(s) :
```



```

    If-match protocol ipv6
Behavior: 2
Accounting enable:
    0 (Packets)
Filter enable: Permit
Marking:
    Remark dscp 3
Classifier: 3
Operator: AND
Rule(s) :
    -none-
Behavior: 3
    -none-

```

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

字段	描述
Direction	QoS策略应用的方向
Green packets	绿色报文的流量统计
Yellow packets	黄色报文的流量统计
Red packets	红色报文的流量统计

其它显示信息解释请参见 [表 1-1](#) 和 [表 1-3](#)。

1.3.4 display qos policy interface

display qos policy interface 命令用来显示接口上 QoS 策略的配置信息和运行情况。

【命令】

```
display qos policy interface [ interface-type interface-number ] [ inbound
| outbound ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
```

【参数】

interface-type interface-number: 指定接口类型和接口编号。如果未指定本参数，将显示所有接口上 QoS 策略的配置信息和运行情况。

inbound: 显示入方向 QoS 策略的配置信息和运行情况。

outbound: 显示出方向 QoS 策略的配置信息和运行情况。

【使用指导】

如果未指定显示方向，则同时显示出入两个方向 QoS 策略的配置信息和运行情况。

【举例】

显示对接口 GigabitEthernet1/0/1 接收到的报文应用 QoS 策略的配置信息和运行情况。

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

```
Interface: GigabitEthernet1/0/1
```

```
Direction: Inbound
```

```
Policy: 1
```

```
Classifier: 1
```

```
Matched : 0 (Packets) 0 (Bytes)
```

```
5-minute statistics:
```

```
Forwarded: 0/0 (pps/bps)
```

```
Dropped : 0/0 (pps/bps)
```

```
Operator: AND
```

```
Rule(s) :
```

```
If-match acl 2000
```

```
Behavior: 1
```

```
Marking:
```

```
Remark dscp 3
```

```
Committed Access Rate:
```

```
CIR 112 (kbps), CBS 51200 (Bytes), EBS 512 (Bytes)
```

```
Green action : pass
```

```
Yellow action : pass
```

```
Red action : discard
```

```
Green packets : 0 (Packets) 0 (Bytes)
```

```
Yellow packets: 0 (Packets) 0 (Bytes)
```

```
Red packets : 0 (Packets) 0 (Bytes)
```

```
Classifier: 2
```

```
Matched : 0 (Packets) 0 (Bytes)
```

```
5-minute statistics:
```

```
Forwarded: 0/0 (pps/bps)
```

```
Dropped : 0/0 (pps/bps)
```

```
Operator: AND
```

```
Rule(s) :
```

```
If-match protocol ipv6
```

```
Behavior: 2
```

```
Accounting enable:
```

```
0 (Packets)
```

```
Filter enable: Permit
```

```
Marking:
```

```
Remark dscp 3
```

```
Classifier: 3
```

```
Matched : 0 (Packets) 0 (Bytes)
```

```
5-minute statistics:
```

```
Forwarded: 0/0 (pps/bps)
```

```
Dropped : 0/0 (pps/bps)
```

```
Operator: AND
```

```
Rule(s) :
```

```
-none-
```

```
Behavior: 3
```

```
-none-
# 显示所有接口上 QoS 策略的配置信息和运行情况。
<Sysname> display qos policy interface
Interface: GigabitEthernet1/0/1
  Direction: Inbound
  Policy: a
  Classifier: a
    Operator: AND
    Rule(s) :
      If-match any
  Behavior: a
  Mirroring:
    Mirror to the interface: GigabitEthernet1/0/2
  Committed Access Rate:
    CIR 112 (kbps), CBS 51200 (Bytes), EBS 0 (Bytes)
    Green action : pass
    Yellow action : pass
    Red action   : discard
    Green packets : 0 (Packets)
    Red packets  : 0 (Packets)

Interface: GigabitEthernet1/0/3
  Direction: Inbound
  Policy: a
  Classifier: a
    Operator: AND
    Rule(s) :
      If-match any
  Behavior: a
  Mirroring:
    Mirror to the interface: GigabitEthernet1/0/4
  Committed Access Rate:
    CIR 112 (kbps), CBS 51200 (Bytes), EBS 0 (Bytes)
    Green action : pass
    Yellow action : pass
    Red action   : discard
    Green packets : 0 (Packets)
    Red packets  : 0 (Packets)
```

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

字段	描述
Direction	QoS策略应用的方向
Matched	符合分类规则的数据包数目
5-minute statistics	最近5分钟的流速统计信息
Forwarded	符合分类规则的成功转发报文在统计周期内的平均速率
Dropped	符合分类规则的丢弃报文在统计周期内的平均速率

字段	描述
Green packets	绿色报文的流量统计
Yellow packets	黄色报文的流量统计
Red packets	红色报文的流量统计

其它显示信息解释请参见 [表 1-1](#) 和 [表 1-3](#)。

1.3.5 display qos policy user-profile

display qos policy user-profile 命令用来显示用户上线后 User Profile 下应用的 QoS 策略的信息和运行情况。

【命令】

```
display qos policy user-profile [ name profile-name ] [ user-id user-id ]
[ slot slot-number ] [ inbound | outbound ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

name *profile-name*: 指定 User Profile 的名称，为 1~31 个字符的字符串，只能包含英文字母 [a-z,A-Z]、数字、下划线，且必须以英文字母开始，区分大小写。User Profile 的名称必须全局唯一。如果未指定本参数，将显示所有 User Profile 下应用的 QoS 策略的信息和运行情况。

user-id *user-id*: 表示在线用户的 ID，为系统所分配，取值范围为十六进制数 0~fffffffe。若未指定本参数，则显示所有用户在 User Profile 下应用的 QoS 策略的信息和运行情况。

slot *slot-number*: 显示指定成员设备上指定用户在 User Profile 下应用的 QoS 策略的信息和运行情况，*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，将显示所有成员设备上的在线用户上指定用户在 User Profile 下应用的 QoS 策略的信息和运行情况。

inbound: 显示入方向 QoS 策略的配置信息和运行情况。

outbound: 显示出方向 QoS 策略的配置信息和运行情况。

【使用指导】

如果未指定显示方向，则同时显示出入两个方向 QoS 策略的配置信息和运行情况。

【举例】

显示指定全局用户（从聚合口等全局口上线的用户）在 User Profile 下应用 QoS 策略的配置信息和运行情况。

```
<Sysname> display qos policy user-profile name abc user-id 30000000 inbound
User-Profile: abc
  User ID: 0x30000000(global)
  Direction: Inbound
```

```

Policy: p1
Classifier: default-class
  Matched : 0 (Packets) 0 (Bytes)
  Operator: AND
  Rule(s) :
    If-match any
  Behavior: be
    -none-

```

显示指定的非全局用户在 **User Profile** 下应用 **QoS** 策略的配置信息和运行情况。

```
<Sysname> display qos policy user-profile name abc user-id 30000001 inbound
```

```
User-Profile: abc
```

```
slot 2:
```

```

User ID: 0x30000001(local)
Direction: Inbound
Policy: p1
Classifier: default-class
  Matched : 0 (Packets) 0 (Bytes)
  Operator: AND
  Rule(s) :
    If-match any
  Behavior: be
    -none-

```

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

字段	描述
User-Profile	User Profile名称
User ID	上线用户的ID
global	该用户从聚合口等全局口上线
local	该用户从物理口上线
Mirror to the interface	镜像到接口
CIR	承诺信息速率，单位为kbps
CBS	承诺突发尺寸，也就是容纳突发流量的令牌桶深度，单位为byte
EBS	超出突发尺寸，在双令牌桶算法中超出突发流量超过承诺突发流量的部分，单位为byte
PIR	峰值信息速率
Direction	QoS策略应用的方向
Matched	符合分类规则的数据包数目
Green packets	绿色报文的流量统计
Yellow packets	黄色报文的流量统计
Red packets	红色报文的流量统计

其它显示信息解释请参见 [表 1-1](#) 和 [表 1-3](#)。

1.3.6 display qos vlan-policy

display qos vlan-policy 命令用来显示基于 VLAN 应用 QoS 策略的配置信息和运行情况。

【命令】

```
display qos vlan-policy { name policy-name | vlan [ vlan-id ] } [ slot slot-number ] [ inbound | outbound ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【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，区分大小写。

vlan *vlan-id*: 显示指定 VLAN 上应用 QoS 策略的信息。*vlan-id* 为指定 VLAN 的 ID 号，取值范围为 1~4094。

inbound: 显示入方向 QoS 策略的配置信息和运行情况。

outbound: 显示出方向 QoS 策略的配置信息和运行情况。

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* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示主设备上基于 VLAN 应用 QoS 策略的信息。

【使用指导】

如果未指定显示方向，则同时显示出入两个方 QoS 策略的配置信息和运行情况。

【举例】

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: AND
      Rule(s) :
        If-match acl 2000
      Behavior: 1
        Marking:
          Remark dscp 3
    Classifier: 2
      Operator: AND
      Rule(s) :
        If-match protocol ipv6
      Behavior: 2
```

```

Accounting enable:
    0 (Packets)
Filter enable: Permit
Marking:
    Remark dscp 3
Classifier: 3
Operator: AND
Rule(s) :
    -none-
Behavior: 3
    -none-

```

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

字段	描述
Direction	QoS策略应用的方向

其它显示信息解释请参见 [表 1-1](#) 和 [表 1-3](#)。

1.3.7 qos apply policy (interface view)

qos apply policy 命令用来在接口上应用 QoS 策略。

undo qos apply policy 命令用来取消接口上应用的 QoS 策略。

【命令】

```

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

```

【缺省情况】

未应用 QoS 策略。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

policy-name: 策略名，为 1~31 个字符的字符串，区分大小写。

inbound: 入方向应用 QoS 策略。

outbound: 出方向应用 QoS 策略。

【举例】

将 QoS 策略 USER1 应用到接口 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

```

1.3.8 qos apply policy (user profile view)

qos apply policy 命令用来在 User Profile 下应用策略。

undo qos apply policy 命令用来取消 User Profile 下应用的策略。

【命令】

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

【缺省情况】

未在 User Profile 下应用 QoS 策略。

【视图】

User Profile 视图

【缺省用户角色】

network-admin

【参数】

inbound: 入方向应用 QoS 策略。

outbound: 出方向应用 QoS 策略。

policy-name: 策略名, 为 1~31 个字符的字符串。

【使用指导】

User Profile 被删除将导致其下引用的 QoS 策略被删除。

User Profile 视图下应用的 QoS 策略不能为空, 因为应用空策略的 User Profile 不能被激活, 且 QoS 策略中的流行为只支持 **car** 和 **accounting** 动作。

【举例】

```
# 对设备发送的上线用户 user 的流量应用策略 test (该策略已经建立)。  
<Sysname> system-view  
[Sysname] user-profile user  
[Sysname-user-profile-user] qos apply policy test outbound
```

1.3.9 qos apply policy global

qos apply policy global 命令用来全局应用 QoS 策略。

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

【命令】

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

【缺省情况】

未在全局应用 QoS 策略。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

policy-name: 策略名，为 1~31 个字符的字符串，区分大小写。

inbound: 入方向应用 QoS 策略。

outbound: 出方向应用 QoS 策略。

【使用指导】

全局应用的 QoS 策略对全部流量生效。

【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
```

1.3.10 qos policy

qos policy 命令用来创建一个策略，并进入策略视图。如果指定的策略已经存在，则直接进入策略视图。

undo qos policy 命令用来删除一个策略。

【命令】

```
qos policy policy-name  
undo qos policy policy-name
```

【缺省情况】

不存在策略。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

policy-name: 策略名，为 1~31 个字符的字符串，区分大小写。

【使用指导】

如果策略已经被应用，则不允许删除该策略，需要先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。

【举例】

定义一个名为 user1 的 QoS 策略。

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

【相关命令】

- `classifier behavior`
- `qos apply policy`
- `qos apply policy global`
- `qos vlan-policy`

1.3.11 qos vlan-policy

`qos vlan-policy` 命令用来在 VLAN 上应用 QoS 策略。

`undo qos vlan-policy` 命令用来取消 VLAN 上应用的 QoS 策略。

【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 }
```

【缺省情况】

未在 VLAN 上应用 QoS 策略。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

policy-name: 策略名称，为 1~31 个字符的字符串，区分大小写。

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: 入方向应用 QoS 策略。

outbound: 出方向应用 QoS 策略。

【举例】

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

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

```
[Sysname] qos vlan-policy test vlan 200 300 400 500 inbound
```

1.3.12 reset qos policy global

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

【命令】

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

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

inbound: 清除入方向 QoS 策略的统计信息。

outbound: 清除出方向 QoS 策略的统计信息。

【使用指导】

如果未指定清除方向，则同时清除出入两个方向 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
```

1.3.13 reset qos vlan-policy

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

【命令】

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

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

vlan *vlan-id*: 指定 VLAN。*vlan-id* 为指定 VLAN 的 ID 号，取值范围为 1~4094。

inbound: 清除入方向 QoS 策略的统计信息。

outbound: 清除出方向 QoS 策略的统计信息。

【使用指导】

如果未指定方向，则同时清除出入两个方向 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

2.1 优先级映射表配置命令

2.1.1 display qos map-table

`display qos map-table` 命令用来显示优先级映射表的配置情况。

【命令】

`display qos map-table [dot1p-lp | dscp-dot1p | dscp-dscp]`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

表2-1 优先级映射表

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

【使用指导】

如果未指定表的类型，将显示所有映射表的配置情况。

【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2-2 display qos map-table 命令显示信息描述表

字段	描述
MAP-TABLE NAME	映射表的名称
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

import 命令用来配置指定优先级映射表的映射关系。

undo import 命令用来删除配置的优先级映射表的映射关系，恢复其为缺省的映射关系。

【命令】

```
import import-value-list export export-value
undo import { import-value-list | all }
```

【缺省情况】

优先级映射表的映射关系请参见配置指导中的附录 B。

【视图】

优先级映射表视图

【缺省用户角色】

network-admin

【参数】

import-value-list: 输入值列表。

export-value: 输出值。

all: 删除配置地该映射表的所有映射关系，恢复其为缺省的映射关系。

【举例】

配置 802.1p 优先级到本地优先级映射表的映射关系，与 802.1p 优先级 4、5 相对应的本地优先级为 1。

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

【相关命令】

- **display qos map-table**

2.1.3 qos map-table

qos map-table 命令用来进入指定的优先级映射表视图。

【命令】

```
qos map-table { dot1p-lp | dscp-dot1p | dscp-dscp }
```

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

其它参数请参见 [表 2-1](#)。

【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]
```

【相关命令】

- `display qos map-table`
- `import`

2.2 端口优先级信任模式配置命令

2.2.1 display qos trust interface

`display qos trust interface` 命令用来显示端口优先级信任模式信息和端口优先级的信息。

【命令】

```
display qos trust interface [ interface-type interface-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface-type interface-number: 指定的接口类型和接口编号。如果未指定本参数，将显示所有接口的端口优先级信任模式信息。

【举例】

显示端口优先级信任模式信息。

```
<Sysname> display qos trust interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
Port priority trust information
Port priority:4
Port priority trust type: dscp
```

表2-3 display qos trust interface 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号构成
Port priority trust information	端口优先级信任信息
Port priority	端口优先级
Port priority trust type	端口优先级信任类型，取值为： <ul style="list-style-type: none"> • dot1p: 802.1p 优先级 • dscp: DSCP 优先级 • none: 不信任任何优先级

2.2.2 qos trust

qos trust 命令用来配置端口优先级信任模式。

undo qos trust 命令用来恢复缺省情况。

【命令】

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

【缺省情况】

设备不信任报文携带的优先级，会使用端口优先级作为报文的 802.1p 优先级进行优先级映射。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【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。

【举例】

在接口 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
```

【相关命令】

```
display qos trust interface
```

2.3 端口优先级配置命令

2.3.1 qos priority

qos priority 命令用来配置端口的端口优先级。

undo qos priority 命令用来恢复端口优先级为缺省值。

【命令】

```
qos priority priority-value  
undo qos priority
```

【缺省情况】

端口优先级的值为 0。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

priority-value: 端口优先级值。取值范围为 0~7。

【举例】

配置接口 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
```

【相关命令】

- **display qos trust interface**

3 流量整形和限速

3.1 流量整形配置命令

3.1.1 display qos gts interface

display qos gts interface 命令用来显示接口的流量整形配置情况。

【命令】

display qos gts interface [*interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface-type interface-number: 指定接口类型和接口编号。如果未指定本参数，将显示所有接口的流量整形配置情况。

【举例】

显示所有接口的流量整形配置情况。

```
<Sysname> display qos gts interface
Interface: GigabitEthernet1/0/1
Rule: If-match queue 1
      CIR 512 (kbps), CBS 51200 (Bytes)
```

表3-1 display qos gts 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号结合在一起组成
Rule	匹配规则
CIR	承诺信息速率，单位为kbps
CBS	承诺突发尺寸，单位为byte

3.1.2 qos gts

qos gts 命令用来在接口上配置流量整形。

undo qos gts 命令用来取消接口上流量整形的配置。

【命令】

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

【缺省情况】

未配置流量整形。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

queue queue-id: 对队列上的数据包进行流量整形。*queue-id* 为匹配的队列号, 取值范围为 0~7。

cir committed-information-rate: 承诺信息速率, 单位为 kbps。Eth 端口的取值范围为 8~102400, GE 端口的取值范围为 8~1048576, 10GE 端口的取值范围为 8~10485760, 用户配置的数值必须是 8 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, 缺省取值为与 $62.5 \times \text{committed-information-rate}$ 的乘积最接近且不小于该乘积值的 512 的整数倍, 但是最大值不能超过 16777216。
- 如果指定 **cbs** 参数, 取值范围 512~16777216 且必须为 512 的整数倍。

【举例】

在接口 GigabitEthernet1/0/1 上对队列 1 中的报文进行流量整形。正常流速为 6400kbps, 突发流量为 51200bytes。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] qos gts queue 1 cir 6400 cbs 51200
```

3.2 限速配置命令

3.2.1 display qos lr interface

display qos lr interface 命令用来显示接口上的限速配置情况。

【命令】

```
display qos lr interface [ interface-type interface-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface-type interface-number: 指定接口类型和接口编号。如果未指定本参数，将显示所有接口的限速配置情况。

【举例】

显示所有接口的接口限速配置情况。

```
<Sysname> display qos lr interface
Interface: GigabitEthernet1/0/1
Direction: outbound
CIR 2000 (kbps), CBS 20480 (Bytes)
```

表3-2 display qos lr 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号结合在一起组成
Direction	接口限速应用的方向
CIR	承诺信息速率，单位为kbps
CBS	承诺突发尺寸，单位为byte

3.2.2 qos lr

qos lr 命令用来配置接口限速。

undo qos lr 命令用来取消接口配置的限速。

【命令】

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

【缺省情况】

未配置限速。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

inbound: 入方向限速。

outbound: 出方向限速。

cir committed-information-rate: 承诺信息速率，单位为 kbps。Eth 端口的取值范围为 8～102400，GE 端口的取值范围为 8～1048576，10GE 端口的取值范围为 8～10485760，用户配置的数值必须是 8 的倍数。

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

如果不指定 **cbs** 参数，缺省取值为与 $62.5 \times committed\text{-}information\text{-}rate$ 的乘积最接近且不小于该乘积值的 512 的整数倍，但是最大值不能超过 134217728。

- 如果指定 **cbs** 参数，取值范围 512~134217728 且必须为 512 的整数倍。

【举例】

对接口 GigabitEthernet1/0/1 上出方向的报文进行限速。正常流速为 256kbps，突发流量为 51200bytes，以后速率小于等于 256kbps 时正常发送，速率大于 256kbps 时，将进行限速。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos lr outbound cir 256 cbs 51200
```

4 拥塞管理

4.1 拥塞管理公共配置命令

4.1.1 display qos queue interface

display qos queue interface 命令用来显示接口上队列配置情况和统计信息。

【命令】

display qos queue interface [*interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface-type interface-number: 指定接口类型和接口编号。如果未指定本参数，将显示所有接口的接口队列配置情况和运行统计信息。

【举例】

显示所有接口下的队列信息。

```
<Sysname> display qos queue interface
Interface: GigabitEthernet1/0/1
  Output queue: Strict Priority queuing
Interface: GigabitEthernet1/0/2
  Output queue: Strict Priority queuing
Interface: GigabitEthernet1/0/3
  Output queue: Strict Priority queuing
Interface: GigabitEthernet1/0/4
  Output queue: Strict Priority queuing
Interface: GigabitEthernet1/0/5
  Output queue: Strict Priority queuing
Interface: GigabitEthernet1/0/6
  Output queue: Strict Priority queuing
```

表4-1 display qos queue 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组成
Output queue	当前出队列的相关信息
Queue ID	队列号
Group	分组号，说明队列属于哪一个分组

字段	描述
Weight	各个队列的调度权重，当前WRR队列调度权重的计算方式为按照每次轮询可发送的报文个数进行计算，N/A表示该队列采用SP调度算法

4.2 严格优先级队列配置命令

4.2.1 display qos queue sp interface

display qos queue sp interface 命令用来显示接口的 SP（Strict Priority，严格优先级）队列配置情况。

【命令】

display qos queue sp interface [*interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface-type interface-number: 指定接口类型和接口编号。如果未指定本参数，将显示所有接口的 SP 队列配置情况。

【举例】

显示 GigabitEthernet1/0/1 的严格优先级队列配置情况。

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

表4-2 display qos queue sp 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组成
Output queue	当前出队列类型

4.2.2 qos sp

qos sp 命令用来在接口上配置严格优先队列。

undo qos sp 命令用来恢复缺省情况。

【命令】

qos sp

undo qos sp

【缺省情况】

接口采用 WRR 调度算法，各队列按照每次轮询可发送的报文个数进行计算。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【举例】

在接口 GigabitEthernet1/0/1 上应用 SP 模式的队列调度。

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

【相关命令】

- **display qos queue sp interface**

4.3 加权轮询队列配置命令

4.3.1 display qos queue wrr interface

display qos queue 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。

【命令】

display qos queue wrr interface [*interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface-type interface-number：指定接口类型和接口编号。如果未指定本参数，将显示所有接口的 WRR 队列配置情况。

【举例】

显示接口 GigabitEthernet1/0/1 的 WRR 队列配置情况。

```
<Sysname> display qos queue wrr interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
Output queue: Weighted Round Robin queuing
Queue ID      Queue name    Group      Weight
-----
0             be           1          1
```

1	af1	1	1
2	af2	1	1
3	af3	1	1
4	af4	1	1
5	ef	1	1
6	cs6	1	1
7	cs7	sp	N/A

表4-3 display qos queue wrr 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组成
Output queue	当前出队列类型
Queue ID	队列号
Queue name	队列名称
Group	分组号，说明队列属于哪一个分组
Weight	各个队列的调度权重，当前WRR队列调度权重的计算方式为按照每次轮询可发送的报文个数进行计算，N/A表示该队列采用SP调度算法

4.3.2 qos wrr

qos wrr 命令用来在接口上开启 WRR 队列。

undo qos wrr 命令用来恢复缺省情况。

【命令】

```
qos wrr weight
undo qos wrr weight
```

【缺省情况】

接口采用 WRR 调度算法，各队列按照每次轮询可发送的报文个数进行计算。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

weight：表示按照每次轮询可发送的报文个数进行计算。

【使用指导】

必须先使用 **qos wrr** 命令在接口上开启 WRR 队列，然后才能进行 WRR 配置。

【举例】

```
# 在接口 GigabitEthernet1/0/1 上开启 WRR 队列，并按照每次轮询可发送的报文个数进行计算。
<Sysname> system-view
```



```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wrr weight
```

【相关命令】

- **display qos queue wrr interface**

4.3.3 qos wrr weight

qos wrr weight 命令用来配置 WRR 队列或修改 WRR 队列的参数。

undo qos wrr 命令用来恢复指定队列的缺省情况。

【命令】

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

【缺省情况】

所有队列均处于 WRR 调度组 1 中，调度权重从 0 到 7 分别为 1、2、3、4、5、9、13、15，各队列按照每次轮询可发送的报文个数进行计算。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

queue-id: 队列序号。取值范围为 0~7 或 [表 4-4](#) 中的关键字。

表4-4 queue-id 数字和关键字对应表

queue-id 数字	queue-id 关键字
0	be
1	af1
2	af2
3	af3
4	af4
5	ef
6	cs6
7	cs7

group 1: 表示该队列属于 WRR 优先组，目前仅支持 1 个 WRR 调度组。

weight: 表示按照每次轮询可发送的报文个数进行计算。

schedule-value: 配置队列的调度权重，取值范围为 1~15。

【使用指导】

必须先使用 **qos wrr** 命令在接口上开启 WRR 队列，然后才能进行本配置。

【举例】

在接口 GigabitEthernet1/0/1 上应用 WRR 队列，并按照每次轮询可发送的报文个数数进行计算，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
```

【相关命令】

- **display qos queue wrr interface**
- **qos wrr**

4.3.4 qos wrr group sp

qos wrr group sp 命令用来配置队列加入 SP 组，采用严格优先级调度算法。

undo qos wrr group sp 命令用来取消将队列加入 SP 组。

【命令】

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

【缺省情况】

当接口使用 WRR 队列时，所有队列均处于 WRR 调度组 1 中。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

queue-id：队列序号。取值范围为 0~7 或 [表 4-4](#) 中的关键字。

【使用指导】

本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。调度时先调度 SP 组，然后调度其他 WRR 优先组。

收到流量的队列中，最低优先级的队列不能加入 SP 组，否则该队列不能进行调度。

【举例】

在接口 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 weight
[Sysname-GigabitEthernet1/0/1] qos wrr 0 group sp
```

【相关命令】

- **display qos queue wrr interface**

- qos wrr

4.4 队列调度策略配置命令

4.4.1 display qos qmprofile configuration

display qos qmprofile configuration 命令用来显示队列调度策略的配置情况。

【命令】

display qos qmprofile configuration [*profile-name*] [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

profile-name: 队列调度策略名称, 为 1~31 个字符的字符串, 区分大小写。如果未指定本参数, 则显示所有队列调度策略的配置情况。

slot slot-number: 显示指定成员设备的队列调度策略的配置情况。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数, 则显示主用设备的队列调度策略的配置情况。

【举例】

显示队列调度策略 myprofile 的配置情况。

```
<Sysname> display qos qmprofile configuration myprofile
Queue management profile: myprofile (ID 1)
Queue ID  Type  Group   Schedule   Schedule   Min        Max
           unit    value    bandwidth  bandwidth
-----
be         SP    N/A     N/A        N/A        N/A        N/A
af1        SP    N/A     N/A        N/A        N/A        N/A
af2        SP    N/A     N/A        N/A        N/A        N/A
af3        SP    N/A     N/A        N/A        N/A        N/A
af4        SP    N/A     N/A        N/A        N/A        N/A
ef         SP    N/A     N/A        N/A        N/A        N/A
cs6        SP    N/A     N/A        N/A        N/A        N/A
cs7        SP    N/A     N/A        N/A        N/A        N/A
```

表4-5 display qos qmprofile configuration 命令显示信息描述表

字段	描述
Queue management profile	队列调度策略名称
Queue ID	队列号
Type	队列调度类型, 包括SP（严格优先级）、WRR（加权轮询调度）
Group	优先组, N/A表示无效, 取值只能为1

字段	描述
Schedule unit	队列调度单位，取值只能为weight，N/A表示无效
Schedule vlaue	<ul style="list-style-type: none"> Weight 表示报文个数 N/A 表示无效
Min Bandwidth	最小保证带宽，N/A表示无效
Max bandwidth	（设备暂不支持）最大带宽值，N/A表示无效

4.4.2 display qos qmprofile interface

display qos qmprofile interface 命令用来显示接口的队列调度策略的配置情况。

【命令】

display qos qmprofile interface [*interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface-type interface-number: 指定接口类型和接口编号。如果未指定本参数，将显示所有接口的队列调度策略的配置情况。

【举例】

显示指定接口的队列调度策略的配置情况。

```
<Sysname> display qos qmprofile interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
Direction: Outbound
Queue management profile: myprofile
```

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

字段	描述
Interface	接口名称
Direction	队列调度策略应用的方向
Queue management profile	队列调度策略名称

4.4.3 qos apply qmprofile

qos apply qmprofile 命令用来在接口出方向上应用队列调度策略。

undo qos apply qmprofile 命令用来恢复缺省情况。

【命令】

```
qos apply qmprofile profile-name
undo qos apply qmprofile
```

【缺省情况】

接口上未应用队列调度策略。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

profile-name: 队列调度策略名称，为 1~31 个字符的字符串，区分大小写。

【使用指导】

每个接口只能应用一个队列调度策略。

【举例】

在接口 GigabitEthernet1/0/1 出方向上应用队列调度策略 myprofile。

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

【相关命令】

- **display qos qmprofile interface**

4.4.4 qos qmprofile

qos qmprofile 命令用来创建用户自定义的队列调度策略，并进入相应的队列调度策略视图。如果指定的队列调度策略已经存在，则直接进入该队列调度策略视图。

undo qos qmprofile 命令用来删除用户自定义的队列调度策略。

【命令】

```
qos qmprofile profile-name
undo qos qmprofile profile-name
```

【缺省情况】

不存在用户自定义的队列调度策略。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

profile-name: 队列调度策略名称，为 1~31 个字符的字符串，区分大小写。

【使用指导】

如果需要删除已经应用到接口的队列调度策略，必须先应用的位置上取消对该队列调度策略的应用，然后再删除该队列调度策略。

【举例】

创建队列调度策略 **myprofile**，并进入队列调度策略视图。

```
<Sysname> system-view
[Sysname] qos qmprofile myprofile
[Sysname-qmprofile-myprofile]
```

【相关命令】

- **display qos qmprofile interface**
- **queue**

4.4.5 queue

queue 命令用来配置队列调度参数。

undo queue 命令用来取消队列调度参数的配置。

【命令】

```
queue queue-id { sp | wrr group group-id weight schedule-value }
undo queue queue-id
```

【缺省情况】

队列调度策略的内容是所有队列均采用 SP 方式调度。

【视图】

队列调度策略视图

【缺省用户角色】

network-admin

【参数】

queue-id: 队列序号。取值范围为 0~7 或 [表 4-4](#) 中的关键字。

sp: 配置队列为严格优先级调度。

wrr: 配置队列为加权轮询调度。

group group-id: 优先组号。取值只能为 1。

weight: 表示按照每次轮询可发送的报文个数进行计算。

schedule-value: 配置队列的调度权重。取值范围为 1~15。

【举例】

创建自定义的队列调度策略 **myprofile**，并配置队列 0 为严格优先级调度。

```
<Sysname> system-view
[Sysname] qos qmprofile myprofile
[Sysname-qmprofile-myprofile] queue 0 sp
```

创建自定义的队列调度策略 **myprofile**，并配置队列 1 为加权轮询调度，权重为 10，分组为 1。

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

```
[Sysname] qos qmprofile myprofile
[Sysname-qmprofile-myprofile] queue 1 wrr group 1 weight 10
```

【相关命令】

- **display qos qmprofile interface**
- **qos qmprofile**

4.5 端口队列统计配置命令

4.5.1 display qos queue-statistics interface outbound

display qos queue-statistics interface outbound 命令用来显示端口队列出方向的统计信息。

【命令】

```
display qos queue-statistics interface [ interface-type interface-number ]  
outbound
```

【视图】

任意视图

【缺省用户角色】

```
network-admin  
network-operator
```

【参数】

interface-type interface-number: 指定接口类型和接口编号。如果未指定本参数，将显示所有接口的队列出方向统计信息。

【举例】

显示接口 GigabitEthernet1/0/1 的队列出方向统计信息。

```
<Sysname> display qos queue-statistics interface gigabitethernet 1/0/1 outbound  
Interface: GigabitEthernet1/0/1  
Direction: outbound  
Forwarded: 0 packets, 0 bytes  
Dropped: 0 packets, 0 bytes  
Queue 0  
Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps  
Dropped: 0 packets, 0 bytes  
Current queue length: 0 packets  
Queue 1  
Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps  
Dropped: 0 packets, 0 bytes  
Current queue length: 0 packets  
Queue 2  
Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps  
Dropped: 0 packets, 0 bytes  
Current queue length: 0 packets
```

Queue 3
Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
Dropped: 0 packets, 0 bytes
Current queue length: 0 packets

Queue 4
Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
Dropped: 0 packets, 0 bytes
Current queue length: 0 packets

Queue 5
Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
Dropped: 0 packets, 0 bytes
Current queue length: 0 packets

Queue 6
Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
Dropped: 0 packets, 0 bytes
Current queue length: 0 packets

Queue 7
Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
Dropped: 0 packets, 0 bytes
Current queue length: 0 packets

表4-7 display qos queue-statistics interface outbound 命令显示信息描述表

字段	描述
Interface	端口队列统计的端口
Direction	端口队列统计的方向
Forwarded	转发的数据包数目和字节数
Dropped	丢弃的数据包数目和字节数
Queue 0、Queue 1、Queue 2、Queue 3、Queue 4、Queue 5、Queue 6、Queue 7	某端口队列统计信息
Current queue length	当前队列长度

【相关命令】

reset counters interface（接口管理命令参考/以太网接口）

5 聚合CAR

5.1 聚合CAR配置命令

5.1.1 car name

car name 命令用来配置聚合 CAR 动作。

undo car 用来恢复缺省情况。

【命令】

car name *car-name*

undo car

【缺省情况】

未配置聚合 CAR 动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

car-name: 聚合 CAR 的名称，首字符需要以字母开头，为 1~31 个字符的字符串，区分大小写。

【举例】

配置流行为 be1 的聚合 CAR 动作为 aggcar-1。

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

```
[Sysname] traffic behavior be1
```

```
[Sysname-behavior-be1] car name aggcar-1
```

【相关命令】

- **display qos car name**
- **display traffic behavior user-defined**

5.1.2 display qos car name

display qos car name 命令用来显示聚合 CAR 的配置和统计信息。

【命令】

display qos car name [*car-name*]

【视图】

任意视图

【缺省用户角色】

network-admin

【参数】

car-name: 聚合 CAR 的名称，首字符需要以字母开头，为 1~31 个字符的字符串，区分大小写。
显示指定聚合 CAR 的配置和统计信息。如果未指定本参数，将显示所有聚合 CAR 的配置和统计信息。

【举例】

```
# 显示聚合 CAR 的配置和统计信息。
<Sysname> display qos car name
Name: a
Mode: aggregative
  CIR 32 (kbps) CBS: 2048 (Bytes) PIR: 888 (kbps) EBS: 0 (Bytes)
  Green action : pass
  Yellow action: pass
  Red action   : discard
Slot 0:
  Green packets: 0 (Packets), 0 (Bytes)
  Yellow packets: 0 (Packets), 0 (Bytes)
  Red packets  : 0 (Packets), 0 (Bytes)
Slot 1:
  Green packets: 0 (Packets), 0 (Bytes)
  Yellow packets: 0 (Packets), 0 (Bytes)
  Red packets  : 0 (Packets), 0 (Bytes)
Slot 2:
  Apply failed
```

表5-1 display qos car name 命令显示信息描述表

字段	描述
Name	聚合CAR的名称
Mode	聚合CAR的类型，取值为aggregative（聚合CAR）
CIR CBS PIR EBS	流量监管流量的参数配置
Green action	对绿色报文的动作 <ul style="list-style-type: none">discard: 丢弃报文pass: 允许报文通过
Yellow action	对黄色报文的动作 <ul style="list-style-type: none">discard: 丢弃报文pass: 允许报文通过
Red action	对红色报文的动作 <ul style="list-style-type: none">discard: 丢弃报文pass: 允许报文通过
Green packets	绿色报文的流量统计
Yellow packets	黄色报文的流量统计

字段	描述
Red packets	红色报文的流量统计

5.1.3 qos car

qos car 命令用来配置聚合 CAR。

undo qos car 命令用来取消聚合 CAR 的配置。

【命令】

```
qos car car-name aggregative cir committed-information-rate [ cbs
committed-burst-size [ ebs excess-burst-size ] ] [ green action | red action
| yellow action ] *
qos car car-name aggregative cir committed-information-rate [ cbs
committed-burst-size ] pir peak-information-rate [ ebs excess-burst-size ]
[ green action | red action | yellow action ] *
undo qos car car-name
```

【缺省情况】

未配置聚合 CAR。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

car-name: 聚合 CAR 的名称，首字符需要以字母开头，为 1~31 个字符的字符串，区分大小写。

cir committed-information-rate: 承诺信息速率，单位为 kbps。取值范围为 8~160000000。

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

- 如果不指定 **cbs** 参数，缺省取值为与 $62.5 \times \text{committed-information-rate}$ 的乘积最接近且不小于该乘积值的 512 的整数倍，但是最大值不能超过 256000000。
- 如果指定 **cbs** 参数，取值范围 512~256000000 且必须为 512 的整数倍。

ebs excess-burst-size: 过度突发尺寸，单位为 byte。

配置 **pir** 参数后：

- 如果不指定 **ebs**，则 **ebs** 缺省取值为与 $62.5 \times \text{peak-information-rate}$ 的乘积最接近且不小于 512 的整数倍，但是最大值不能超过 256000000。
- 如果指定 **ebs**，取值范围 0~256000000 且必须为 512 的整数倍。

未配置 **pir** 参数时，**ebs** 的取值范围为 0~256000000 且必须为 512 的整数倍。

pir peak-information-rate: 峰值速率，单位为 kbps。取值范围为 8~160000000。

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

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

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**。

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-dot1p-pass new-cos:** 设置新的 802.1P 报文的优先级值，并允许数据包通过，取值范围为 0~7。
- **remark-dscp-pass new-dscp:** 设置报文新的 DSCP 值，并允许数据包通过，取值范围为 0~63；用文字表示时，可以选取 **af11**、**af12**、**af13**、**af21**、**af22**、**af23**、**af31**、**af32**、**af33**、**af41**、**af42**、**af43**、**cs1**、**cs2**、**cs3**、**cs4**、**cs5**、**cs6**、**cs7**、**default**、**ef**。

【使用指导】

聚合 CAR 配置需要在策略中引用后才能生效。

配置了聚合 CAR 的 QoS 策略不支持在出方向应用。

不配置峰值速率表示所配置的是单速率流量监管，否则表示双速率流量监管。

【举例】

配置聚合 CAR 采取的 CAR 参数取值，**cir** 取值为 25600，**cbs** 取值为 512000，对于红色报文采取丢弃的动作。

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

```
[Sysname] qos car aggcar-1 aggregative cir 25600 cbs 512000 red discard
```

【相关命令】

- **display qos car name**

5.1.4 reset qos car name

reset qos car name 命令用来清除聚合 CAR 的统计信息。

【命令】

```
reset qos car name [ car-name ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

car-name: 聚合 CAR 的名称，首字符需要以字母开头，为 1~31 个字符的字符串，区分大小写。清除指定聚合 CAR 的统计信息。如果未指定本参数，将清除所有聚合 CAR 的统计信息。

【举例】

清除聚合 CAR aggcar-1 的统计信息。

```
<Sysname> reset qos car name aggcar-1
```


目 录

1 数据缓冲区.....	1-1
1.1 数据缓冲区配置命令.....	1-1
1.1.1 buffer apply	1-1
1.1.2 buffer queue guaranteed	1-1
1.1.3 buffer shared	1-2
1.1.4 buffer total-shared.....	1-3
1.1.5 burst-mode enable	1-4
1.1.6 display buffer	1-5

1 数据缓冲区

1.1 数据缓冲区配置命令

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。

burst-mode enable 与 **buffer apply** 命令互斥，用户在开启 **Burst** 功能后，不能应用手工配置数据缓冲区的相应配置，反之亦然。如果已经使用某一种方式进行了配置，则必须先取消该方式的配置之后，才能使用另外一种方式进行配置。

1.1.1 buffer apply

buffer apply 命令用来应用用户对数据缓冲区所做的配置。

undo buffer apply 命令用来恢复缺省情况。

【命令】

```
buffer apply
undo buffer apply
```

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

用户对数据缓冲区进行配置后，必须使用 **buffer apply** 命令进行应用，这些配置才能生效。
配置被应用后就不能被修改，需要先取消应用，再修改、应用，新的配置才能生效。

【举例】

应用用户对数据缓冲区所做的配置。

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

1.1.2 buffer queue guaranteed

buffer queue guaranteed 命令用来配置队列最多可使用的固定区域的比例。

undo buffer queue guaranteed 命令用来取消指定队列最多可使用的固定区域的比例的配置。

【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
```


【缺省情况】

每个队列最多可使用的 **cell** 资源中固定区域比例为 12%。

每个队列最多可使用的 **packet** 资源中固定区域的比例为 12%。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

egress: 表示对发送数据缓冲区进行配置。

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示配置所有成员设备。

cell: 表示 **cell** 资源。

packet: 表示 **packet** 资源。

queue-id: 需要配置的队列编号，取值范围为 0~7。

ratio ratio: 队列最多可使用的缓存大小占整个固定区域的大小的百分比。该参数的取值范围为 0~100。

【使用指导】

缺省情况下，所有队列均分固定区域，但用户也可以使用该命令调整指定队列最多可使用的固定区域的比例，其它未配置的队列则均分剩余的固定区域。

配置该命令后，系统就与给队列预留指定大小的空间，即便该队列没有报文存储需求，其他队列也不能抢占。所有队列所配置的固定区域大小之和，不应超过可配置的总固定区域大小，否则配置失败。

【举例】

配置队列 0 最多可使用的 **cell** 固定区域的比例为整个 **cell** 固定缓冲区大小的 20%。

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

```
[Sysname] buffer egress cell queue 0 guaranteed ratio 20
```

1.1.3 buffer shared

buffer shared 命令用来配置端口或指定队列最多可使用的共享区域的比例。

undo buffer shared 命令用来取消端口或指定队列最多可使用的共享区域的比例的配置。

【命令】

```
buffer egress [ slot slot-number ] { cell | packet } [ queue queue-id ] shared  
ratio ratio
```

```
undo buffer egress [ slot slot-number ] { cell | packet } [ queue queue-id ]  
shared
```

【缺省情况】

每个端口最多可使用的 **packet** 资源中共享区域的比例为 10%。

每个端口最多可使用的 **cell** 资源中共享区域的比例为 10%。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

egress: 表示对发送数据缓冲区进行配置。

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示配置所有成员设备。

cell: 表示 cell 资源。

packet: 表示 packet 资源。

queue-id: 需要配置的队列编号，取值范围为 0~7。未指定该参数时，表示配置所有端口可使用的共享区域的比例。

ratio ratio: 队列的最大共享缓存占用比，以百分数形式表示。该参数的取值范围为 0~100。

【使用指导】

缺省情况下，所有端口或队列均分共享区域，但用户也可以调整端口或指定队列最多可使用的共享区域的比例，其它未配置的队列最多可使用的共享区域的比例仍遵循缺省值。最终，各端口或队列最多可使用的共享区域的大小将由芯片根据 **buffer shared** 配置，以及实际需要收发报文的数量决定。

【举例】

配置队列 0 在 cell 资源中的最大共享缓存占用比为 10%。

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

```
[Sysname] buffer egress cell queue 0 shared ratio 10
```

1.1.4 buffer total-shared

buffer total-shared 命令用来配置数据缓冲区中共享区域的比例。

undo buffer total-shared 命令用来取消数据缓冲区中共享区域的比例的配置。

【命令】

```
buffer egress [ slot slot-number ] { cell | packet } total-shared ratio ratio
```

```
undo buffer egress [ slot slot-number ] { cell | packet } total-shared
```

【缺省情况】

cell 缓冲区中共享区域所占比例为 52%，packet 缓冲区中共享区域所占比例为 50%。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

egress: 表示对发送数据缓冲区进行配置。

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示配置所有成员设备。

cell: 表示 cell 资源。

packet: 表示 packet 资源。

ratio ratio: 缓冲区中共享区域所占的比例，以百分数形式表示。该参数的取值范围为 0~100。

【使用指导】

设备上整个数据缓冲区的大小是固定的，用户配置共享区域的大小后，其余部分将自动成为固定区域。

【举例】

配置当前设备 cell 资源中的共享区域所占比例为 50%。

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

```
[Sysname] buffer egress cell total-shared ratio 50
```

1.1.5 burst-mode enable

burst-mode enable 命令用来开启数据缓冲区自动分配功能。

undo burst-mode enable 命令用来关闭数据缓冲区自动分配功能。

【命令】

burst-mode enable

undo burst-mode enable

【缺省情况】

数据缓冲区自动分配功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

在下列情况下，开启数据缓冲区自动分配功能可以提高报文缓存功能和降低报文丢包率：

- 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设备，由低速链路转发出去；或者报文从相同速率的多个接口同时进入设备，由一个相同速率的接口转发出去。

开启数据缓冲区自动分配功能后，如下缓冲区的比例将发生变化：

- 每个队列最多可使用缓冲区中固定区域比例。
- 每个队列最多可使用缓冲区中共享区域的比例。
- 缓冲区中共享区域所占比例。

开启前后的具体变化情况，可通过 **display buffer** 命令查看。

开启数据缓冲区自动分配功能前后，设备缓冲区的分配情况会有较大的变化，可以通过 **display buffer** 命令查看开启前后设备数据缓冲区的分配情况。

【举例】

开启数据缓冲区自动分配功能。

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

1.1.6 display buffer

display buffer 命令用来显示数据缓冲区的比例。

【命令】

```
display buffer [ slot slot-number ] [ queue [ queue-id ] ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
```

【参数】

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示所有成员设备。

queue queue-id: 显示队列最多可使用的固定区域的比例以及队列最多可使用的共享区域的比例，queue-id 的取值范围为 0~7。指定 queue-id 时，显示指定队列的相关信息；不指定 queue-id 时，显示所有队列的相关信息。未指定本参数时，显示共享区域的比例。

【举例】

```
# 显示数据缓冲区的比例。
<Sysname> display buffer
Slot  Type      Eg(Total-shared , Shared)
1      packet   0 , 20
1      cell     0 , 20

      Eg: Size of the sending buffer
Total-shared: Size of the shared buffer for all ports
      Shared: Size of the maximum shared buffer per port
      Unit: Ratio

# 显示队列最多可使用的固定区域的比例以及队列最多可使用的共享区域的比例。
<Sysname> display buffer queue
Slot  Queue      Type      Eg(Guaranteed , Shared)
1      0-7        packet   12 , --
1      0-7        cell     12 , --

      Eg: Size of the sending buffer
      Guaranteed: Size of the minimum guaranteed buffer per queue
      Shared: Size of the maximum shared buffer per queue
      Unit: Ratio
```

表1-1 display buffer 命令显示信息描述表

字段	描述
Type	缓冲区类型，包括packet资源和cell资源

字段	描述
Queue	队列ID，范围为0~7
Eg	Egress，出方向的数据缓冲区配置
(Total-shared , Shared)	Total-shared表示所有端口共享区域的比例 Shared表示每个端口专用的共享区域的大小
(Guaranteed , Shared)	Guaranteed表示每个队列最多可使用的固定区域的比例 Shared表示每个队列最多可使用的共享区域的比例。如果显示为“--”字符串，则表示设备不支持该数据缓冲区
Unit	数据缓冲区的单位，为%

目 录

1 时间段.....	1-1
1.1 时间段配置命令.....	1-1
1.1.1 display time-range	1-1
1.1.2 time-range	1-2

1 时间段

1.1 时间段配置命令

1.1.1 display time-range

display time-range 命令用来显示时间段的配置和状态信息。

【命令】

```
display time-range { time-range-name | all }
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
```

【参数】

time-range-name: 显示指定名称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。

【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 11/23/2010 Tuesday

Time-range : t4 (Inactive)
 10:00 to 12:00 Mon
 14:00 to 16:00 Wed
from 00:00 1/1/2011 to 00:00 1/1/2012
from 00:00 6/1/2011 to 00:00 7/1/2011
```

表1-1 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">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

1.1.2 time-range

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。如果指定的时间段已经创建，则本命令可以修改时间段的时间范围。

undo time-range 命令用来删除一个时间段。

【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 ]
```

【缺省情况】

不存在时间段。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

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

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

days: 指定周期时间段在每周的周几生效。本参数可输入多次，但后输入的值不能与此前输入的值完全重叠（譬如输入 6 后不允许再输入 **Sat**，但允许再输入 **off-day**），系统将取各次输入值的并集作为最终值（譬如依次输入 1、**Wed** 和 **working-day** 之后，最终生效的时间将为每周的工作日）。本参数可输入的形式如下：

- 数字：取值范围为 0~6，依次表示周日~周六；
- 周几的英文缩写（从周日到周六依次为 **Sun**、**Mon**、**Tue**、**Wed**、**Thu**、**Fri** 和 **Sat**）；
- 工作日（**working-day**）：表示从周一到周五；
- 休息日（**off-day**）：表示周六和周日；
- 每日（**daily**）：表示一周七天。

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

to time2 date2: 指定绝对时间段的结束时间。**time2** 的格式为 hh:mm，取值范围为 00:00~24:00。**date2** 的格式为 MM/DD/YYYY 或 YYYY/MM/DD。MM 表示月，取值范围为 1~12；DD 表示日，取值范围取决于所输入的月份；YYYY 表示年，取值范围为 1970~2100。结束时间必须大于起始

时间。若未指定本参数，绝对时间段的结束时间将为系统可表示的最晚时间，即 2100 年 12 月 31 日 24 点 0 分。

【使用指导】

如果指定名称的时间段不存在，则创建一个新的时间段（最多 1024 个）；如果指定名称的时间段已存在，则对旧时间段进行修改，即在其原有内容的基础上叠加新的内容。

在一个时间段中，可以使用以下两种方式定义时间范围：

- 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。

如果一个时间段中同时包含以上两种时间范围，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。例如在一个时间段中定义周期时间段为每周一的 8 点到 12 点，定义绝对时间段为 2015 年全年，那么该时间段的生效时间范围为 2015 年全年内每周一的 8 点到 12 点。

一个时间段内可包含一或多个周期时间段（最多 32 个）和绝对时间段（最多 12 个），当包含有多个周期时间段和绝对时间段时，系统将先分别取各周期时间段的并集和各绝对时间段的并集，再取这两个并集的交集作为该时间段最终生效的时间范围。

【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 08:00 to 18:00 working-day
```

创建名为 t2 的时间段，其时间范围为 2011 年全年。

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

```
[Sysname] time-range t2 from 00:00 1/1/2011 to 24:00 12/31/2011
```

创建名为 t3 的时间段，其时间范围为 2011 年全年内每周休息日的 8 点到 12 点。

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

```
[Sysname] time-range t3 08:00 to 12:00 off-day from 00:00 1/1/2011 to 24:00 12/31/2011
```

创建名为 t4 的时间段，其时间范围为 2011 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 10:00 to 12:00 1 from 00:00 1/1/2011 to 24:00 1/31/2011
```

```
[Sysname] time-range t4 14:00 to 16:00 3 from 00:00 6/1/2011 to 24:00 6/30/2011
```

【相关命令】

- **display time-range**