H3C SecPath L100/L1000/L5000/ADE 插卡负载均衡产品

ACL 和 QoS 命令参考(V7)

新华三技术有限公司
http://www.h3c.com

资料版本：6W401-20200915
产品版本：

L5000-C/L5000-S/L5000-E	E8142
L5030/L5060/L5080	E8516
L5000-SV100	E1101
L5000-AK535	E8516
L1000-C/L1000-S/L1000-M/L1000-E	E8139
L1030/L1050/L1070/L1090	E1101
L1000-AK310/L1000-AK320/L1000-AK330	E8139
L1000-AK390	E1101
L100-C	E9522
LSU1ADECEA0	E8144
LSWM1ADED0/LSQM1ADEDSC0	E8534

前 言

本命令参考主要介绍配置 ACL 和 QoS 功能时涉及的各种命令。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... }*	表示从多个选项中至少选取一个。
[x | y | ...]*	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

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

3. 各类标志

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

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

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	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 ACL配置命令

1.1.1 accelerate

accelerate 命令用来开启 ACL 规则的加速匹配功能。

undo accelerate 命令用来恢复缺省情况。

【命令】

accelerate

undo accelerate

【缺省情况】

ACL 规则的加速匹配功能处于关闭状态。

【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

context-admin

【使用指导】

只有系统 ACL 资源充足时加速匹配功能才会生效。

只有 ACL 中的所有规则都支持加速匹配时，执行本命令才能成功开启该 ACL 的加速匹配功能。

成功开启本功能后，再去修改或添加新的规则时，可能会由于 ACL 资源不足或新增规则不支持加速导致 ACL 加速匹配失败。

当设备支持软件加速，并开启本功能后，添加、删除和修改规则时，并不会立即加速，而是延迟一定时间后加速。如果在该时间内，规则又发生变化，则重新计时。当 ACL 中的规则小于等于 100 条时，此时间为 2 秒；当 ACL 中的规则大于 100 条时，此时间为 20 秒。

【举例】

开启 ACL 2000 的加速匹配功能。

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

【相关命令】

- **display acl accelerate**

1.1.2 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】

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* }

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

context-admin

【参数】

ipv6：指定 ACL 类型为 IPv6 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。

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】

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 报文的消息类型和消息码信息、VPN 实例、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**

1.1.3 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

context-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。

【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
```

1.1.4 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，同时开启报文的首包上送功能。

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。报文首包上送功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-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)

1.1.5 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

context-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)

1.1.6 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

context-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**

1.1.7 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

context-admin

context-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。

【举例】

显示所有 IPv4 ACL 的配置和运行情况。

```
<Sysname> display acl all
Basic IPv4 ACL 2001, 2 rules, match-order is auto,
This is an IPv4 basic ACL.
ACL's step is 5
ACL accelerated
 rule 5 permit source 1.1.1.1 0 (5 times matched)
 rule 5 comment This rule is used on GigabitEthernet1/0/1.
 rule 10 permit source object-group permit (5 times matched)
Advanced IPv4 ACL 3001, 1 rule,
ACL's step is 5
 rule 0 permit ip source 1.1.1.0 0.0.0.255 destination 3.3.3.0 0.0.0.255 (Dynamic)
```

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，ACL的类型包括： • Basic IPv4 ACL：表示 IPv4 基本 ACL • Advanced IPv4 ACL：表示 IPv4 高级 ACL • Basic IPv6 ACL：表示 IPv6 基本 ACL • Advanced IPv6 ACL：表示 IPv6 高级 ACL • MAC ACL：表示二层 ACL
2 rules	该ACL内包含的规则数量

字段	描述
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
ACL accelerated	该ACL开启了加速功能
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 10 permit source object-group permit	规则10的具体内容，源地址为对象组
5 times matched	该规则匹配的次数为5（仅统计软件ACL的匹配次数，当匹配次数为0时不显示本字段）
rule 5 comment This rule is used on GigabitEthernet1/0/1.	规则5的描述信息
Dynamic	该规则由应用模块动态添加

1.1.8 display acl accelerate

display acl accelerate 命令用来显示 ACL 的加速状态。

【命令】

display acl accelerate { **summary** [**ipv6** | **mac**] | **verbose** [**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

context-admin

context-operator

【参数】

summary：显示 ACL 加速的概要信息。

verbose：显示 ACL 加速的详细信息。

ipv6：显示 IPv6 ACL 的加速状态。

mac：显示二层 ACL 的加速状态。

acl-number：显示指定编号的 ACL 的加速状态。*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*：显示指定名称的 ACL 的加速状态。*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*：显示指定成员设备的 ACL 加速信息，该设备必须为加速芯片所在成员设备，*slot-number* 表示设备在 IRF 中的成员编号。

【使用指导】

指定 **verbose** 关键字时，将会显示成功开启加速匹配功能的 ACL 及其中已配置的规则，但对于未开启或未成功开启加速匹配功能的 ACL，将不会显示出来。

【举例】

显示加速概要信息。

```
<Sysname> display acl accelerate summary
Basic IPv4 ACL 2000
```

1.1.9 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**] | **zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*] } [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-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，将显示除 VA（Virtual Access，虚拟访问）接口外所有接口上 ACL 在报文过滤中的应用情况。有关 VA 接口的详细介绍，请参见“PPP 和 PPPoE 配置指导”中的“PPP”。

当接口类型为以太网接口时，不需要指定 **slot** 参数。

zone-pair security [**source** *source-zone-name* **destination** *destination-zone-name*]：显示指定安全域间实例上 ACL 在报文过滤中的应用情况。*source-zone-name*：表示安全域间实例源安全域的名称，为 1～31 个字符的字符串，不区分大小写。*destination-zone-name*：表示安全域间实例目的安全域的名称，为 1～31 个字符的字符串，不区分大小写。

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 (Failed)
  IPv4 default action: Deny
  IPv6 default action: Deny
  MAC default action: Deny
```

显示安全域间实例源域 office 到目的域 library 上 ACL 在报文过滤中的应用情况。

```
<Sysname> display packet-filter zone-pair security source office destination library
Zone-pair: source office destination library
  IPv4 ACL 2001
  IPv4 ACL 2002
```

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
Zone-pair	ACL在指定安全域间实例上的应用情况
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
IPv4 default action	报文过滤的缺省动作，包括： • 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： • 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

字段	描述
MAC default action	报文过滤的缺省动作，包括： • 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

1.1.10 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** } [**default** | [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] | **zone-pair security source** *source-zone-name* **destination** *destination-zone-name* [[**ipv6**] { *acl-number* | **name** *acl-name* }] } [**brief**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-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。

zone-pair security source *source-zone-name* **destination** *destination-zone-name*：显示指定安全域间实例上的统计信息。*source-zone-name*：表示安全域间实例源安全域的名称，为 1～31 个字符的字符串，不区分大小写。*destination-zone-name*：表示安全域间实例目的安全域的名称，为 1～31 个字符的字符串，不区分大小写。

inbound：显示入方向上的统计信息。

outbound：显示出方向上的统计信息。

default：显示报文过滤缺省动作的统计信息。

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】

如果未指定任何可选参数，将显示全部 ACL 在报文过滤中应用的统计信息。

【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
   From 2011-06-04 10:25:21 to 2011-06-04 10:35:57
   rule 0 permit source 2.2.2.2 0 counting (2 packets, 256 bytes)
   rule 5 permit source 1.1.1.1 0 counting (Failed)
   rule 10 permit vpn-instance test counting (No resource)
   Totally 2 packets 256 bytes permitted, 0 packets 0 bytes denied
   Totally 100% permitted, 0% denied

  IPv6 ACL 2000

  MAC ACL 4000
   rule 0 permit

  IPv4 default action: Deny

  IPv6 default action: Deny
  MAC default action: Deny
```

显示安全域间实例源域 office 到目的域 library 上 IPv4 高级 ACL 3001 在报文过滤中应用的统计信息。

```
<Sysname> display packet-filter statistics zone-pair security source office destination
library 3001
Zone-pair: source office destination library
IPv4 ACL 3001
   rule 0 permit source 2.2.2.2 0
   rule 5 permit source 1.1.1.1 0 counting (2 packets)
   rule 10 permit vpn-instance test (Failed)
   Totally 2 packets 256 bytes permitted, 0 packets 0 bytes denied
   Totally 100% permitted, 0% denied
```

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
Zone-pair	在指定安全域间实例上应用的统计信息

字段	描述
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
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 1.1.1.10 (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： • 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： • 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： • 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**

1.1.11 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

context-admin

context-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。

【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 counting (2 packets,  256 bytes)
   rule 5 permit source 1.1.1.1 0
   rule 10 permit vpn-instance test
   Totally 2 packets 256 bytes permitted, 0 packets 0 bytes 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 256 bytes permitted, 0 packets 0 bytes 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

字段	描述
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, 256 bytes	该规则匹配了2个包，共256字节（当匹配的包个数为0时不显示本字段）
Totally 2 packets 256 bytes permitted, 0 packets 0 bytes denied	该ACL允许和拒绝符合条件报文的个数及字节数
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**

1.1.12 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* }] | **zone-pair security source** *source-zone-name* **destination** *destination-zone-name* [[**ipv6**] { *acl-number* | **name** *acl-name* }] } [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-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。

zone-pair security source *source-zone-name* **destination** *destination-zone-name*：显示指定安全域间实例上 ACL 在报文过滤中的详细应用情况。*source-zone-name*：表示安全域间实例源安全域的名称，为 1～31 个字符的字符串，不区分大小写。*destination-zone-name*：表示安全域间实例目的安全域的名称，为 1～31 个字符的字符串，不区分大小写。

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。

【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)
   rule 10 permit vpn-instance test (Failed)

  IPv6 ACL 2000
   rule 0 permit

  MAC ACL 4000

  IPv4 default action: Deny

  IPv6 default action: Deny

  MAC default action: Deny
```

#显示安全域间实例源域 office 到目的域 library 上全部 ACL 在报文过滤中的详细应用情况。

```
<Sysname> display packet-filter verbose zone-pair security source office destination library
Zone-pair: source office destination library
  IPv4 ACL 2001
   rule 0 permit
   rule 5 permit source 1.1.1.1 0
   rule 10 permit vpn-instance test
```

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
Zone-pair	ACL在指定安全域间实例上的详细应用情况
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
rule 5 permit source 1.1.1.10 (Failed)	规则5应用失败
IPv4 default action	报文过滤的缺省动作，包括： • 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： • 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： • 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

1.1.13 packet-filter (interface view)

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** }

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】

接口视图

【缺省用户角色】

network-admin

context-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。

【使用指导】

此功能在聚合成员端口上不生效。

【举例】

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

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

【相关命令】

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

1.1.14 packet-filter (zone pair view)

packet-filter 命令用来在安全域间实例上应用 ACL 进行报文过滤。

undo packet-filter 命令用来取消在安全域间实例上应用 ACL 进行报文过滤。

【命令】

packet-filter [**ipv6**] { *acl-number* | **name** *acl-name* }

undo packet-filter [**ipv6**] { *acl-number* | **name** *acl-name* }

【缺省情况】

在安全域间实例上没有应用 ACL 进行报文过滤。

【视图】

安全域间实例视图

【缺省用户角色】

network-admin

context-admin

【参数】

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

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。

【举例】

应用 IPv4 基本 ACL 2002 对源安全域 office 到目的安全域 library 的安全域间实例收到的报文进行过滤。

```
<Sysname> system-view
[Sysname] zone-pair security source office destination library
[Sysname-zone-pair-security-office-library] packet-filter 2002
```

【相关命令】

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

1.1.15 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

context-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**

1.1.16 reset acl counter

reset acl counter 命令用来清除 ACL 的统计信息。

【命令】

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

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

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 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。

all：清除指定类型中全部 ACL 的统计信息。

name *acl-name*：清除指定名称 ACL 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。

【举例】

清除 IPv4 基本 ACL 2001 的统计信息。

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

【相关命令】

- **display acl**

1.1.17 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** } [**default** | [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] | **zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*] [**ipv6**] { *acl-number* | **name** *acl-name* }] }

【视图】

用户视图

【缺省用户角色】

network-admin

context-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。

zone-pair security [**source** *source-zone-name* **destination** *destination-zone-name*]：清除指定接口上的统计信息。*source-zone-name*：表示安全域间实例源安全域的名称，为 1～31 个字符的字符串，不区分大小写。*destination-zone-name*：表示安全域间实例目的安全域的名称，为 1～31 个字符的字符串，不区分大小写。

inbound：清除入方向上的统计信息。

outbound：清除出方向上的统计信息。

default：清除缺省动作在报文过滤中应用的统计信息。

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 **default**、*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。

【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
```

清除在源安全域 office 到目的安全域 library 的安全域间实例上 IPv4 基本 ACL 2001 在报文过滤中应用的统计信息。

```
<Sysname> reset packet-filter statistics zone-pair security source office destination
library 2001
```

【相关命令】

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

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

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

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

context-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 **gre**（47）、**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 1-6 所示的规则信息参数。

表1-6 规则信息参数

参数	类别	作用	说明
source { **object-group** *address-group-name* | *source-address source-wildcard* | **any** }	源地址信息	指定ACL规则的源地址信息	*address-group-name*：源地址对象组的名称 *source-address*：源IP地址 *source-wildcard*：源IP地址的通配符掩码（为0表示主机地址） **any**：任意源IP地址
destination { **object-group** *address-group-name* | *dest-address dest-wildcard* | **any** }	目的地址信息	指定ACL规则的目的地址信息	*address-group-name*：目的地址对象组的名称 *dest-address*：目的IP地址 *dest-wildcard*：目的IP地址的通配符掩码（为0表示主机地址） **any**：任意目的IP地址
counting	统计	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
precedence *precedence*	报文优先级	指定IP优先级	*precedence*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 *tos*	报文优先级	指定ToS优先级	*tos*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）

参数	类别	作用	说明
dscp *dscp*	报文优先级	指定DSCP优先级	*dscp*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	仅对分片报文的非首个分片有效，而对非分片报文和分片报文的首个分片无效	若未指定该参数，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	表示记录规则匹配报文的日志信息，包括匹配报文的规则和匹配报文的个数	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 *time-range-name*	时间段	指定本规则生效的时间段	*time-range-name*：时间段的名称，为1～32个字符的字符串，不区分大小写。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”
vpn-instance *vpn-instance-name*	VPN实例	对指定VPN实例中的报文有效	*vpn-instance-name*：MPLS L3VPN的VPN实例名称，为1～31个字符的字符串，区分大小写 若未指定本参数，表示该规则对非VPN报文有效，对VPN报文无效

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

表1-7 TCP/UDP 特有的规则信息参数

参数	类别	作用	说明
source-port { **object-group** *port-group-name* | *operator port1* [*port2*] }	源端口	定义TCP/UDP报文的源端口信息	*port-group-name*：端口对象组的名称 *operator*为操作符，取值可以为**lt**（小于）、**gt**（大于）、**eq**（等于）、**neq**（不等于）或者**range**（在范围内，包括边界值）。只有操作符**range**需要两个端口

参数	类别	作用	说明
destination-port { **object-group** *port-group-name* | *operator port1* [*port2*] }	目的端口	定义TCP/UDP报文的目的端口信息	号做操作数，其它的只需要一个端口号做操作数 *port1*、*port2*：TCP或UDP的端口号，用数字表示时，取值范围为0～65535；用字符表示时，TCP端口号可以选取**chargen**（19）、**bgp**（179）、**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）、**mobilip-ag**（434）、**mobilip-mn**（435）、**nameserver**（42）、**netbios-dgm**（138）、**netbios-ns**（137）、**netbios-ssn**（139）、**ntp**（123）、**rip**（520）、**snmp**（161）、**snmptrap**（162）、**sunrpc**（111）、**syslog**（514）、**tacacs-ds**（65）、**talk**（517）、**tftp**（69）、**time**（37）、**who**（513）、**xdmcp**（177）
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	TCP报文标识	定义对携带不同标志位（包括ACK、FIN、PSH、RST、SYN和URG六种）的TCP报文的处理规则	TCP协议特有的参数。表示匹配携带不同标志位的TCP报文，各*value*的取值可为0或1（0表示不携带此标志位，1表示携带此标志位） 对于一条规则中各标志位的配置组合，处理方式为“或”。譬如：当配置为**ack** 0 **psh** 1时，则匹配不携带ACK或携带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，表示匹配携带ACK或RST标志位的TCP连接报文

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

表1-8 ICMP 特有的规则信息参数

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

表1-9 ICMP 消息名称与消息类型和消息码的对应关系

ICMP 消息名称	ICMP 消息类型	ICMP 消息码
echo	8	0
echo-reply	0	0
fragmentneed-DFset	3	4

ICMP 消息名称	ICMP 消息类型	ICMP 消息码
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。

创建的规则若与动态规则的内容完全相同，则会覆盖已有动态规则。

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。

新创建或修改的规则若指定对象组，则该对象组必须存在，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** [*rule-id*] { **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）

1.1.19 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** { **object-group** *address-group-name* | *source-address source-wildcard* | **any** } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

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

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

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

logging：表示记录规则匹配报文的日志信息，包括匹配报文的规则和匹配报文的个数。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 { **object-group** *address-group-name* | *source-address source-wildcard* | **any** }：指定规则的源 IP 地址信息。*address-group-name* 表示源 IP 地址对象组的名称，*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。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”。

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

【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。

新创建或修改的规则若指定对象组，则该对象组必须存在，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** [*rule-id*] { **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 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）

1.1.20 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** { **object-group** *address-group-name* | *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** } | **destination-port** { **object-group** *port-group-name* | *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** { **object-group** *address-group-name* | *source-address source-prefix* | *source-address/source-prefix* | **any** } | **source-port** { **object-group** *port-group-name* | *operator port1* [*port2*] } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

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

undo 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** { **object-group** *address-group-name* | *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** } | **destination-port** { **object-group** *port-group-name* | *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** { **object-group** *address-group-name* | *source-address source-prefix* | *source-address/source-prefix* | **any** } | **source-port** { **object-group** *port-group-name* | *operator port1* [*port2*] } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-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

context-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 **gre**（47）、**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 1-10 所示的规则信息参数。

表1-10 规则信息参数

参数	类别	作用	说明
source { **object-group** *address-group-name* | *source-address source-prefix* | *source-address/source-prefix* | **any** }	源IPv6地址	指定ACL规则的源IPv6地址信息	*address-group-name*：源地址对象组的名称 *source-address*：源IPv6地址 *source-prefix*：源IPv6地址的前缀长度，取值范围1～128 **any**：任意源IPv6地址

参数	类别	作用	说明
destination { **object-group** *address-group-name* | *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** }	目的IPv6地址	指定ACL规则的目的IPv6地址信息	*address-group-name*：目的地址对象组的名称 *dest-address*：目的IPv6地址 *dest-prefix*：目的IPv6地址的前缀长度，取值范围1～128 **any**：任意目的IPv6地址
counting	统计	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
dscp *dscp*	报文优先级	指定DSCP优先级	*dscp*：用数字表示时，取值范围为0～63；用名称表示时，可选取**af11**（10）、**af12**（12）、**af13**（14）、**af21**（18）、**af22**（20）、**af23**（22）、**af31**（26）、**af32**（28）、**af33**（30）、**af41**（34）、**af42**（36）、**af43**（38）、**cs1**（8）、**cs2**（16）、**cs3**（24）、**cs4**（32）、**cs5**（40）、**cs6**（48）、**cs7**（56）、**default**（0）或**ef**（46）
flow-label *flow-label-value*	流标签字段	指定IPv6基本报文头中流标签字段的值	*flow-label-value*：流标签字段的值，取值范围为0～1048575
fragment	报文分片	仅对分片报文的非首个分片有效，而对非分片报文和分片报文的首个分片无效	若未指定本参数，表示该规则对所有报文（包括非分片报文和分片报文的每个分片）均有效
logging	日志操作	表示记录规则匹配报文的日志信息，包括匹配报文的规则和匹配报文的个数	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*]	路由头	指定路由头的类型	*routing-type*：路由头类型的值，取值范围为0～255 若指定了**type** *routing-type*参数，表示仅对指定类型的路由头有效；否则，表示对IPv6所有类型的路由头都有效
hop-by-hop [**type** *hop-type*]	逐跳头	指定逐跳头的类型	*hop-type*：逐跳头类型的值，取值范围为0～255 若指定了**type** *hop-type*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

参数	类别	作用	说明
time-range *time-range-name*	时间段	指定本规则生效的时间段	*time-range-name*：时间段的名称，为1～32个字符的字符串，不区分大小写。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”
vpn-instance *vpn-instance-name*	VPN实例	对指定VPN实例中的报文有效	*vpn-instance-name*：MPLS L3VPN的VPN实例名称，为1～31个字符的字符串，区分大小写 若未指定本参数，表示该规则对非VPN报文有效，对VPN报文无效

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

表1-11 TCP/UDP 特有的规则信息参数

参数	类别	作用	说明
source-port { **object-group** *port-group-name* | *operator port1* [*port2*] }	源端口	定义TCP/UDP报文的源端口信息	*port-group-name*：端口对象组的名称 *operator*：操作符，取值可以为**lt**（小于）、**gt**（大于）、**eq**（等于）、**neq**（不等于）或者**range**（在范围内，包括边界值）。只有**range**操作符需要两个端口号做操作数，其它操作符只需要一个端口号做操作数 *port1*/*port2*：TCP或UDP的端口号，用数字表示时，取值范围为0～65535；用名称表示时，TCP端口号可选取**chargen**（19）、**bgp**（179）、**cmd**（514）、**daytime**（13）、**discard**（9）、**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）、**mobilip-ag**（434）、**mobilip-mn**（435）、**nameserver**（42）、**netbios-dgm**（138）、**netbios-ns**（137）、**netbios-ssn**（139）、**ntp**（123）、**rip**（520）、**snmp**（161）、**snmptrap**（162）、**sunrpc**（111）、**syslog**（514）、**tacacs-ds**（65）、**talk**（517）、**tftp**（69）、**time**（37）、**who**（513）或**xdmcp**（177）
destination-port { **object-group** *port-group-name* | *operator port1* [*port2*] }	目的端口	定义TCP/UDP报文的目的端口信息	
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	TCP报文标识	定义对携带不同标志位（包括ACK、FIN、PSH、RST、SYN和URG六种）的TCP报文的处理规则	TCP协议特有的参数。表示匹配携带不同标志位的TCP报文，各*value*的取值可为0或1（0表示不携带此标志位，1表示携带此标志位） 对于一条规则中各标志位的配置组合，处理方式为“或”。譬如：当配置为**ack** 0 **psh** 1时，则匹配不携带ACK或携带PSH标志位的TCP报文

参数	类别	作用	说明
established	TCP连接建立标识	定义对TCP连接报文的处理规则	TCP协议特有的参数，表示匹配携带ACK或RST标志位的TCP连接报文

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

表1-12 ICMPv6 特有的规则信息参数

参数	类别	作用	说明
icmp6-type { *icmp6-type* *icmp6-code* | *icmp6-message* }	ICMPv6报文的消息类型和消息码	指定本规则中ICMPv6报文的消息类型和消息码信息	*icmp6-type*：ICMPv6消息类型，取值范围为0～255 *icmp6-code*：ICMPv6消息码，取值范围为0～255 *icmp6-message*：ICMPv6消息名称。可以输入的ICMPv6消息名称，及其与消息类型和消息码的对应关系如表1-13所示

表1-13 ICMPv6 消息名称与消息类型和消息码的对应关系

ICMPv6 消息名称	ICMPv6 消息类型	ICMPv6 消息码
echo-reply	129	0
echo-request	128	0
err-Header-field	4	0
frag-time-exceeded	3	1
hop-limit-exceeded	3	0
host-admin-prohib	1	1
host-unreachable	1	3
neighbor-advertisement	136	0
neighbor-solicitation	135	0
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】

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。

创建的规则若与动态规则的内容完全相同，则会覆盖已有动态规则。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。

新创建或修改的规则若指定对象组，则该对象组必须存在，否则将提示出错，并导致该操作失败。

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** [*rule-id*] { **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）

1.1.21 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** { **object-group** *address-group-name* | *source-address source-prefix* | *source-address*/*source-prefix* | **any** } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

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

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

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

logging：表示记录规则匹配报文的日志信息，包括匹配报文的规则和匹配报文的个数。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 { **object-group** *address-group-name* | *source-address source-prefix* | *source-address*/*source-prefix* | **any** }：指定规则的源 IPv6 地址信息。*address-group-name* 表示源 IP 地址对象组的名称，*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。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”。

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

【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。

新创建或修改的规则若指定对象组，则该对象组必须存在，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** [*rule-id*] { **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 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）

1.1.22 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 [*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*] *

【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

context-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。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** [*rule-id*] { **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）

1.1.23 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

context-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**

1.1.24 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*

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

context-admin

【参数】

step-value：表示规则编号的步长值，取值范围为 1～20。

【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 定义类的命令

1.1.1 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

context-admin

context-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

1.1.2 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 [**not**] *match-criteria*

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

context-admin

【参数】

not：不匹配该规则。

match-criteria：类的匹配规则，具体情况如表 1-2 所示。

表1-2 类的匹配规则取值

取值	描述
acl [**ipv6**] { *acl-number* | **name** *acl-name* }	定义匹配ACL的规则 *acl-number*是ACL的序号，IPv4 ACL序号的取值范围是2000～3999，IPv6 ACL序号的取值范围是2000～3999 *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
app-group *group-name*	定义匹配应用组的规则，group-name为应用组的名称。建议引用已创建的应用组；引用未创建的应用组时，无法实现匹配报文的目的。有关创建应用组的详细介绍，请参见“安全配置指导”中的“APR”

取值	描述
application *app-name*	定义匹配应用名的规则，app-name为用户创建的应用名称
any	定义匹配所有数据包的规则
classifier *classifier-name*	定义匹配QoS类的规则，*classifier-name*为类名
customer-dot1p *dot1p-value*&<1-8>	定义匹配内层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
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
inbound-interface *interface-type interface-number*	定义匹配入接口的规则，*interface-type interface-number*为接口类型和接口编号 在“and”模式的流分类中如果配置了本规则，然后将入接口所在单板或子卡拔出，会导致流分类失效，此时如果将单板或子卡恢复，则流分类会重新生效。但如果不恢复单板或子卡，请删除该流分类并按需重新配置。否则，即使再向该流分类中新增其他匹配规则，该流分类也不会生效
ip-precedence *ip-precedence-value*&<1-8>	定义匹配IP优先级的规则，*ip-precedence-value*&<1-8>为IP优先级的列表，IP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
packet-length { **min** *min-value* | **max** *max-value* } *	定义匹配报文长度的规则，*min-value*为匹配报文最小长度的字节数，*max-value*为匹配报文最大长度的字节数 *max-value*必须大于等于*min-value*
protocol *protocol-name*	定义匹配协议的规则，*protocol-name*取值为ip、ipv6
qos-local-id *local-id-value*	定义匹配QoS本地ID值的规则，*local-id-value*为QoS本地ID，取值范围为1～4095
rtp start-port *start-port-number* **end-port** *end-port-number*	定义匹配RTP协议端口的规则。*start-port-number*为起始RTP端口号，取值范围为2000～65535；*end-port-number*为结束RTP端口号，取值范围为2000～65535 用于匹配落在指定RTP端口号范围内的RTP报文，即匹配所有在*start-port-number*与*end-port-number*之间的偶数UDP端口号的报文
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 规则的动作为 **deny** 时，则跳出该 **if-match**，继续进行后续规则的查找。

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
  - if-match classifier classB

【举例】

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

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

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

```
<Sysname> system-view
[Sysname] traffic classifier class2
[Sysname-classifier-class2] if-match source-mac 0050-ba27-bed2
```

定义类 class1 的匹配规则为：匹配内层 VLAN Tag 的 802.1p 优先级为 3。

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

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

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

定义类匹配 IP 协议的报文。

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

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

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

定义类 class1 匹配 QoS 本地 ID 值为 3 的报文。

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

定义类 class1 匹配应用组 multimedia。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match app-group multimedia
```

定义类 class1 匹配应用名 3link。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match application 3link
```

在流分类 class1 中配置匹配报文长度为 100～200 字节的报文。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match packet-length min 100 max 200
```

1.1.3 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

context-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 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

context-admin

【参数】

cir *committed-information-rate*：承诺信息速率。流量的平均速率，取值范围为 8～10000000，单位为 kbps。

cbs *committee-burst-size*：承诺突发尺寸，取值范围为 1000～1000000000，单位为 byte，配置 cir 后，如果不指定 cbs 参数，缺省取值为 62.5 × committed-information-rate。

ebs *excess-burst-size*：超出突发尺寸，取值范围为 0～1000000000，单位为 byte，配置 pir 后，如果不指定 ebs 参数，缺省取值为 62.5 × peak-information-rate。

pir *peak-information-rate*：峰值速率，取值范围为 8～10000000，单位为 kbps，**pir** 和 **cir** 速率单位必须保持一致。

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-prec-pass** *new-precedence*：设置新的 IP 优先级，并允许数据包通过，取值范围为 0～7。

【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
```

1.2.2 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

context-admin

context-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)
      Committed Access Rate:
        CIR 22222 (kbps), CBS 222222222 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
```

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
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

1.2.3 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

context-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
```

1.2.4 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 dot1p *dot1p-value*

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

context-admin

【参数】

dot1p-value：802.1p 优先级，取值范围为 0～7。

【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
```

1.2.5 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 dscp *dscp-value*

undo remark 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

context-admin

【参数】

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

表1-4 DSCP 关键字与值的对应表

关键字	DSCP 值（二进制）	DSCP 值（十进制）
af11	001010	10
af12	001100	12
af13	001110	14
af21	010010	18
af22	010100	20
af23	010110	22
af31	011010	26
af32	011100	28
af33	011110	30
af41	100010	34
af42	100100	36
af43	100110	38
cs1	001000	8

关键字	DSCP 值（二进制）	DSCP 值（十进制）
cs2	010000	16
cs3	011000	24
cs4	100000	32
cs5	101000	40
cs6	110000	48
cs7	111000	56
default	000000	0
ef	101110	46

【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。

【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
```

1.2.6 remark ip-precedence

remark ip-precedence 命令用来重新标记报文的 IP 优先级。

undo remark ip-precedence 命令用来恢复缺省情况。

【命令】

remark ip-precedence *ip-precedence-value*

undo remark ip-precedence

【缺省情况】

未配置重新标记报文 IP 优先级的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip-precedence-value：IP 优先级，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。

【举例】

重新标记报文的 IP 优先级值为 6。

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

1.2.7 remark qos-local-id

remark qos-local-id 命令用来重新标记报文的 QoS 本地 ID 值。

undo remark qos-local-id 命令用来恢复缺省情况。

【命令】

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

undo remark qos-local-id

【缺省情况】

未配置重新标记报文的 QoS 本地 ID 值的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

context-admin

【参数】

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

【使用指导】

一般情况下，在 QoS 策略的入方向对报文的 QoS 本地 ID 值进行标记，在 QoS 策略的出方向根据标记的 QoS 本地 ID 值对报文进行分类以及指定相应的流行为，两者要结合使用。

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】

重新标记报文的 QoS 本地 ID 值为 2。

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

1.2.8 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

context-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**

1.2.9 traffic-policy

traffic-policy 命令用来在父策略流行为视图下应用一个子策略。

undo traffic-policy 命令用来删除关联的子策略。

【命令】

traffic-policy *policy-name*

undo traffic-policy

【缺省情况】

未配置应用子策略的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name：QoS 策略名，为 1～31 个字符的字符串，区分大小写。如果 QoS 策略不存在，则自动创建该 QoS 策略。

【使用指导】

通过在流行为视图下应用子策略，可以实现策略嵌套功能。即由 **traffic classifier** 命令定义的某一类流量，除了执行父策略中定义的行为外，还由子策略再次对该类流量进行分类，并执行子策略中定义的行为。

在配置策略嵌套功能时，请注意：

- 在父策略行为下应用子策略时，最多只能嵌套二层策略，并且不能嵌套自身。
- 一个流行为中至多只能嵌套一个子策略。

嵌套策略支持对 IPv4、IPv6 报文的处理。

如果嵌套策略已经应用在接口上，则不允许删除嵌套的子策略，必须先解除子策略和父策略的嵌套关系。

【举例】

配置策略嵌套，在父策略下应用子策略 child。

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

【相关命令】

- **traffic classifier**
- **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

context-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。

如果 **undo** 命令指定的类为系统预定义类 default-class，表示恢复 default-class 对应的流行为为系统预定义流行为 be，而不是取消对应的流行为。

【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

context-admin

context-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
      Filter enable: Permit
   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 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*] [**slot** *slot-number*] [**inbound** | **outbound**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-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。

slot *slot-number*：显示指定成员设备指定逻辑接口的 QoS 策略的配置信息和运行情况。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示主设备逻辑接口 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
     Filter enable: Permit

  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
      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: b
   Classifier: b
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: b
      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
      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1-6 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
Policy	用户定义的QoS策略名或系统预定义的QoS策略名
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
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、表 1-3 和表 1-5。

1.3.4 qos apply policy

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】

接口视图

【缺省用户角色】

network-admin

context-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】

策略在接口上应用的规则如下：

在应用策略时，如果策略中为确保转发和加速转发的类指定的带宽之和超过接口允许的可用带宽，则在该接口不可应用。如果对接口修改了可用带宽，此时如果策略中为确保转发和加速转发的类指定的带宽之和超过接口允许的可用带宽，则将策略删除。

【举例】

将 QoS 策略 USER1 应用到接口 GigabitEthernet1/0/1 的入方向上。

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

1.3.5 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

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

【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**

1.4 接口流速统计配置命令

1.4.1 qos flow-interval

qos flow-interval 命令用来配置接口流速统计时间。

undo qos flow-interval 命令用来恢复缺省情况。

【命令】

qos flow-interval *interval*

undo qos flow-interval

【缺省情况】

接口流速统计时间为 5 分钟。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

interval：流速统计时间，单位为分钟。取值范围为 1～10。

【使用指导】

配置本命令后，设备将以设置的统计时间为周期，统计周期内经过 QoS 策略流分类后每类报文的发送和丢弃速率，并以 t/5 为刷新周期定期刷新统计速率。

子接口的流速统计时间采用主接口的统计时间。

【举例】

配置接口 GigabitEthernet1/0/1 的流速统计时间为 10 分钟。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos flow-interval 10
```

【相关命令】

- **display qos policy interface**

2 流量监管

2.1 流量监管配置命令

2.1.1 display qos car interface

display qos car interface 命令用来显示接口的流量监管配置情况和统计信息。

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-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监管配置情况和统计信息。

【使用指导】

如果指定接口为 Virtual-Template 接口，将显示继承该 Virtual-Template 接口的所有 Virtual-Access 接口下的流量监管配置情况和统计信息，Virtual-Template 本身无 QoS 信息显示。

【举例】

显示接口 GigabitEthernet1/0/1 的流量监管配置情况和统计信息。

```
<Sysname> display qos car interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
 Direction: inbound
  Rule: If-match any
   CIR 128 (kbps), CBS 5120 (Bytes), PIR 128 (kbps), 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)
```

显示接口 GigabitEthernet1/0/2 的流量监管配置情况和统计信息。

```
<Sysname> display qos car interface gigabitethernet 1/0/2
Interface: GigabitEthernet1/0/2
 Direction: inbound
```

```
Rule: If-match any
 CIR 50 (%), CBS 600 (ms), EBS 0 (ms), PIR 50 (%)
 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)
```

表2-1 display qos car interface 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号结合在一起组成
Direction	流量监管应用的方向
Rule	数据包的匹配规则
CIR	承诺信息速率，单位为kbps
CBS	承诺突发尺寸，单位为byte
EBS	超出突发尺寸，单位为byte
PIR	峰值信息速率，单位为kbps
Green action	对绿色报文的动作
Yellow action	对黄色报文的动作
Red action	对红色报文的动作
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

2.1.2 display qos carl

display qos carl 命令用来显示 CAR 列表。

【命令】

display qos carl [*carl-index*] [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

carl-index：CAR 列表的号码，取值范围为 1～199。如果未指定本参数，将显示所有的 CAR 列表。

slot *slot-number*：显示指定成员设备的 CAR 列表信息，*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 CAR 列表的配置信息。

【举例】

显示 CAR 列表。

```
<Sysname> display qos carl
List  Rules
1     destination-ip-address range 1.1.1.1 to 1.1.1.2 per-address shared-bandwidth
2     destination-ip-address subnet 1.1.1.1 22 per-address shared-bandwidth
4     dscp 1 2 3 4 5 6 7 cs1
5     mac 0000-0000-0000
9     precedence 0 1 2 3 4 5 6 7
10    source-ip-address range 1.1.1.1 to 1.1.1.2
11    source-ip-address subnet 1.1.1.1 31
```

表2-2 display qos carl 命令显示信息描述表

字段	描述
List	CAR列表号码
Rules	数据包的匹配规则

2.1.3 qos car

qos car 命令用来在接口上配置流量监管。

undo qos car 命令用来取消接口上流量监管的配置。

【命令】

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

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

【缺省情况】

未配置流量监管。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

inbound：入方向流量监管。

outbound：出方向流量监管。

any：对所有的 IP 数据包进行流量监管。

acl [**ipv6**] *acl-number*：对匹配 ACL 的数据包进行流量监管。*acl-number* 为 ACL 编号，基本的 ACL 取值范围为 2000～2999，高级的 ACL 取值范围为 3000～3999。若未指定 **ipv6** 关键字，表示 IPv4 ACL；否则表示 IPv6 ACL。

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

cir *committed-information-rate*：承诺信息速率，单位为 kbps。取值范围为 8～10000000。

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。取值范围为 1875～19375000，配置 cir 后，如果不指定 cbs 参数，缺省取值为 62.5 × committed-information-rate。

ebs *excess-burst-size*：过度突发尺寸，单位为 byte。取值范围为 0～19375000，配置 pir 后，如果不指定 ebs 参数，缺省取值为 62.5 × peak-information-rate。

pir *peak-information-rate*：峰值速率，单位为 kbps。取值范围为 8～10000000。

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：

- **continue**：继续由下一个 CAR 策略处理。
- **discard**：丢弃数据包。
- **pass**：允许数据包通过。
- **remark-dot1p-continue** *new-cos*：设置新的 802.1P 报文的优先级值，并继续由下一个 CAR 策略处理，取值范围为 0～7。
- **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-continue** *new-dscp*：设置报文新的 DSCP 值，并继续由下一个 CAR 策略处理，取值范围为 0～63；用文字表示时，可以选取 **af11**、**af12**、**af13**、**af21**、**af22**、**af23**、**af31**、**af32**、**af33**、**af41**、**af42**、**af43**、**cs1**、**cs2**、**cs3**、**cs4**、**cs5**、**cs6**、**cs7**、**default**、**ef**。
- **remark-dscp-pass** *new-dscp*：设置报文新的 DSCP 值，并允许数据包通过，取值范围为 0～63；用文字表示时，可以选取 **af11**、**af12**、**af13**、**af21**、**af22**、**af23**、**af31**、

af32、**af33**、**af41**、**af42**、**af43**、**cs1**、**cs2**、**cs3**、**cs4**、**cs5**、**cs6**、**cs7**、**default**、**ef**。

- **remark-prec-continue** *new-precedence*：设置新的 IP 优先级，并继续由下一个 CAR 策略处理，取值范围为 0～7。
- **remark-prec-pass** *new-precedence*：设置新的 IP 优先级，并允许数据包通过，取值范围为 0～7。

【使用指导】

在同一个接口上重复执行本命令可以配置多个 CAR 策略，策略的执行顺序与配置的先后顺序一致。

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】

在接口 GigabitEthernet1/0/1 的出方向上对满足 ANY 规则的报文进行流量监管。报文正常流速为 200kbps，在第一时间可以有大于正常流量的突发流量通过，以后速率小于等于 200kbps 时正常发送，大于 200kbps 时，报文优先级改为 0 并发送。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos car outbound any cir 200 cbs 5120 ebs 0 green pass red remark-prec-pass 0
```

【相关命令】

- **display qos car interface**
- **qos carl**

2.1.4 qos carl

qos carl 命令用来创建或修改 CAR 列表。

undo qos carl 命令用来删除 CAR 列表。

【命令】

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

undo qos carl *carl-index*

【缺省情况】

未配置 CAR 列表。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

carl-index：CAR 列表号码，取值范围为 1～199。

dscp *dscp-list*：DSCP 取值列表。DSCP 为区分服务编码点，用数字表示时，取值范围为 0～63；用文字表示时，可以选取 **af11**、**af12**、**af13**、**af21**、**af22**、**af23**、**af31**、**af32**、**af33**、**af41**、**af42**、**af43**、**cs1**、**cs2**、**cs3**、**cs4**、**cs5**、**cs6**、**cs7**、**default**、**ef**。可以配置多个 DSCP 值，最多可指定 8 个；如果指定了多个相同的 DSCP 值，系统默认为一个；多个不同的 DSCP 值是或的关系，即只要有一个值匹配，就算匹配这条规则。

mac *mac-address*：16 进制的 MAC 地址。

precedence *precedence-value*：优先级，取值范围为 0～7。可以配置多个 **precedence** 值，最多可指定 8 个；如果指定了多个相同的 **precedence** 值，系统默认为一个；多个不同的 **precedence** 值是或的关系，即只要有一个值匹配，就算匹配这条规则。

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

source-ip-address：基于源 IP 地址的 CAR 列表。

range *start-ip-address* **to** *end-ip-address*：IP 地址段起始地址和 IP 地址段终止地址。*end-ip-address* 必须大于 *start-ip-addres*。**range** 指定的 IP 地址数量上限为 1024。

subnet *ip-address mask-length*：IP 子网地址和 IP 子网地址掩码长度。取值范围为 22～31。

per-address：表示对网段内逐 IP 地址流量进行限速，cir 为各 IP 地址独享的限制带宽，不能被网段内其他 IP 流量共享。如果未指定本参数，将对整个网段的流量进行限速，cir 为该网段内所有 IP 地址带宽之和，各个 IP 地址带宽按照流量大小的比例进行分配。

shared-bandwidth：表示网段内存在流量的 IP 地址均分配置的共享带宽，cir 为该网段内所有 IP 地址的共享带宽，根据当前存在流量的 IP 地址数量，动态平均分配各 IP 地址占用的带宽。

【使用指导】

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

重复执行本命令时，如果 *carl-index* 取值不同，将创建多个 CAR 列表；如果 *carl-index* 取值相同，则表示修改指定 CAR 列表的参数。

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

【举例】

在接口 GigabitEthernet1/0/1 的出方向上应用 CAR 列表 1。CAR 列表 1 是对源地址属于子网 1.1.1.0/24 内每台主机限速 512kbps，网段内各 IP 地址的流量不共享剩余带宽。

```
<Sysname> system-view
[Sysname] qos carl 1 source-ip-address subnet 1.1.1.0 24 per-address
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos car outbound carl 1 cir 512 cbs 5120 ebs 0 green pass red discard
```

在接口 GigabitEthernet1/0/1 的出方向上应用 CAR 列表 2。CAR 列表 2 是对源地址属于 IP 地址段 1.1.2.100～1.1.2.199 内所有主机限速 5Mbps，网段内各 IP 地址的流量共享剩余带宽。

```
<Sysname> system-view
[Sysname] qos carl 2 source-ip-address range 1.1.2.100 to 1.1.2.199 per-address shared-bandwidth
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] qos car outbound carl 2 cir 5120 cbs 51200 ebs 51200 green
pass red discard
```

【相关命令】

- **display qos carl**
- **qos car**

目 录

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

context-admin

context-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，使用英文字母时不区分大小写。

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 00:00:00 1/1/2011 to 00:00:00 1/1/2012
 from 00:00:00 6/1/2011 to 00:00:00 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： • 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

context-admin

【参数】

time-range-name：指定时间段的名称，为 1～32 个字符的字符串，使用英文字母时不区分大小写。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 或 hh:mm:ss，取值范围为 00:00:00～23:59:59。*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 0 秒。

to *time2 date2*：指定绝对时间段的结束时间。*time2* 的格式为 hh:mm 或 hh:mm:ss，取值范围为 00:00:00～24:00:00。*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 0 秒。

【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
```

创建名为 t5 的时间段，其时间范围为 2018 年 1 月 1 日的 8 点到 18 点。

```
<Sysname> system-view
[Sysname] time-range t5 from 08:00:00 1/1/2018 to 18:00:00 1/1/2018
```

【相关命令】

- **display time-range**