# 目 录

# 1 ACL

说明

本文中的“CSPC 单板”指的是单板丝印以“CSPC”开头（如 CSPC-GP48LB）的单板。

## 1.1 ACL配置命令

### 1.1.1 acl

**acl** 命令用来创建一个 ACL，并进入相应的 ACL 视图。

**undo acl** 命令用来删除指定或全部 ACL。

【命令】

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

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

【缺省情况】

不存在任何 ACL。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

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

- 2000～2999：若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL；否则表示 IPv6 基本 ACL。
- 3000～3999：若未指定 **ipv6** 关键字，表示 IPv4 高级 ACL；否则表示 IPv6 高级 ACL。
- 4000～4999：表示二层 ACL（指定 **ipv6** 关键字后不会显示本项）。

**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** 表示按照配置顺序即 ACL 的编号顺序进行规则匹配。缺省情况下，规则的匹配顺序为配置顺序。

**all**：指定全部 ACL。若未指定 **ipv6** 关键字，表示全部 IPv4 基本 ACL、IPv4 高级 ACL 和二层 ACL；否则，表示全部 IPv6 基本 ACL 和 IPv6 高级 ACL。

【使用指导】

- 使用 **acl** 命令时，如果指定编号的 ACL 不存在，则创建该 ACL 并进入其视图，否则直接进入其视图。
- ACL 的名称只能在创建时设置。ACL 一旦创建，便不允许再修改或删除其原有名称。
- 当 ACL 内不存在任何规则时，用户可以使用本命令对该 ACL 的规则匹配顺序进行修改，否则不允许进行修改。

【举例】

# 创建一个编号为 2000 的 IPv4 基本 ACL，并进入其视图。

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

# 创建一个编号为 2001 的 IPv4 基本 ACL，指定其名称为 flow，并进入其视图。

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

【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** ] **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

mdc-admin

【参数】

*source-acl-number*：指定源 ACL 的编号，该 ACL 必须存在。本参数的取值范围及其代表的 ACL 类型如下：

- 2000～2999：若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL；否则表示 IPv6 基本 ACL。
- 3000～3999：若未指定 **ipv6** 关键字，表示 IPv4 高级 ACL；否则表示 IPv6 高级 ACL。
- 4000～4999：表示二层 ACL（指定 **ipv6** 关键字后不会显示本项）。

**name** *source-acl-name*：指定源 ACL 的名称，该 ACL 必须存在。*source-acl-name* 为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。对于基本 ACL 或高级 ACL，若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称，否则表示 IPv6 基本 ACL 或 IPv6 高级 ACL 的名称。

*dest-acl-number*：指定目的 ACL 的编号，该 ACL 必须不存在。若未指定本参数，系统将为目的 ACL 自动分配一个与源 ACL 类型相同且可用的最小编号。本参数的取值范围及其代表的 ACL 类型如下：

- 2000～2999：若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL；否则表示 IPv6 基本 ACL。
- 3000～3999：若未指定 **ipv6** 关键字，表示 IPv4 高级 ACL；否则表示 IPv6 高级 ACL。
- 4000～4999：表示二层 ACL（指定 **ipv6** 关键字后不会显示本项）。

**name** *dest-acl-name*：指定目的 ACL 的名称，该 ACL 必须不存在。*dest-acl-name* 为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 all。若未指定本参数，系统将不会为目的 ACL 设置名称。对于基本 ACL 或高级 ACL，若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称，否则表示 IPv6 基本 ACL 或 IPv6 高级 ACL 的名称。

【使用指导】

- 目的 ACL 的类型要与源 ACL 的类型相同。
- 目的 ACL 的名称只能在复制时设置。目的 ACL 一旦生成，便不允许再修改或删除其原有名称。
- 除了 ACL 的编号和名称不同外，新生成的 ACL（即目的 ACL）的匹配顺序、规则匹配统计功能的使能情况、规则编号的步长、所包含的规则、规则的描述信息以及 ACL 的描述信息等都与源 ACL 的相同。

【举例】

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

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

### 1.1.3 acl logging interval

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

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

【命令】

**acl** [ **ipv6** ] **logging interval** *interval*

**undo acl** [ **ipv6** ] **logging interval**

【缺省情况】

报文过滤日志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

mdc-admin

【参数】

*interval*：若未指定 **ipv6** 关键字，表示 IPv4 报文过滤日志的生成与发送周期，否则表示 IPv6 报文过滤日志的生成与发送周期。取值范围为 0～1440，且必须为 5 的整数倍，0 表示不进行记录，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 进行报文过滤的日志进行记录，且在上述 ACL 中配置规则时必须指定 **logging** 参数。

【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 name

**acl name** 命令用来进入指定名称的 ACL 视图。

【命令】

**acl** [ **ipv6** ] **name** *acl-name*

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

*acl-name*：指定 ACL 的名称，该 ACL 必须存在。*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。对于基本 ACL 或高级 ACL，若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称，否则表示 IPv6 基本 ACL 或 IPv6 高级 ACL 的名称。

【举例】

# 进入已存在的、名称为 flow 的 IPv4 基本 ACL 的视图。

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

# 进入已存在的、名称为 flow 的 IPv6 基本 ACL 的视图。

```
<Sysname> system-view
[Sysname] acl ipv6 name flow
```

```
[Sysname-acl6-basic-2001-flow]
```

【相关命令】

- **acl**

### 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

mdc-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 number 2000
[Sysname-acl-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** ] { *acl-number* | **all** | **name** *acl-name* }

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

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

- 2000～2999：若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL；否则表示 IPv6 基本 ACL。
- 3000～3999：若未指定 **ipv6** 关键字，表示 IPv4 高级 ACL；否则表示 IPv6 高级 ACL。
- 4000～4999：表示二层 ACL（指定 **ipv6** 关键字后不会显示本项）。

**all**：显示全部 ACL 的配置和运行情况。若未指定 **ipv6** 关键字，表示全部 IPv4 基本 ACL、IPv4 高级 ACL 和二层 ACL；否则，表示全部 IPv6 基本 ACL 和 IPv6 高级 ACL。

**name** *acl-name*：显示指定名称的 ACL 的配置和运行情况。*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。对于基本 ACL 或高级 ACL，若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称，否则表示 IPv6 基本 ACL 或 IPv6 高级 ACL 的名称。

【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 IPv4 基本 ACL 2001 的配置和运行情况。

```
<Sysname> display acl 2001
Basic ACL  2001, named flow, 1 rule, match-order is auto,
This is an IPv4 basic ACL.
ACL's step is 5
 rule 5 permit source 1.1.1.1 0
 rule 5 comment This rule is used on GigabitEthernet 3/0/1
```

表1-1 display acl 命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Basic ACL  2001 | 该ACL的类型和编号，ACL的类型包括：<br>• Basic ACL：表示 IPv4 基本 ACL<br>• Advanced ACL：表示 IPv4 高级 ACL<br>• Basic IPv6 ACL：表示 IPv6 基本 ACL<br>• Advanced IPv6 ACL：表示 IPv6 高级 ACL<br>• Ethernet frame ACL：表示二层 ACL |
| named flow | 该ACL的名称为flow，-none-表示没有名称 |
| 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 |

| 字段 | 描述 |
| --- | --- |
| ACL's step is 5 | 该ACL的规则编号的步长值为5 |
| 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 GigabitEthernet 3/0/1. | 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** ] | { **global** | **interface vlan-interface** *vlan-interface-number* } [ **inbound** | **outbound** ] [ **slot** *slot-number* ] }

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

**global**：显示 ACL 在报文过滤中的全局（即所有物理接口）应用情况。

**interface** [ *interface-type interface-number* ]：显示指定接口上 ACL 在报文过滤中的应用情况。*interface-type interface-number* 表示接口类型和接口编号，这里的接口类型不包括 VLAN 接口。若未指定接口类型和接口编号，将显示除 VLAN 接口以外的所有接口上 ACL 在报文过滤中的应用情况。

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

**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*：显示指定单板上 ACL 在报文过滤中的应用情况，*slot-number* 表示单板所在的槽位号。若未指定本参数，将显示主用主控板上 ACL 在报文过滤中的应用情况。

【使用指导】

若未指定 **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 GigabitEthernet3/0/1 入方向上 ACL 在报文过滤中的应用情况。

```
<Sysname> display packet-filter interface gigabitethernet 3/0/1 inbound
Interface: GigabitEthernet3/0/1
```

```
In-bound policy:
  ACL 2003, Hardware-count
  Default action: Deny
```

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 |
| In-bound policy | ACL在入方向上的应用情况 |
| Out-bound policy | ACL在出方向上的应用情况 |
| ACL 2003 | IPv4基本ACL 2003应用成功 |
| Hardware-count | 规则匹配统计功能应用成功 |
| Default action | 报文过滤缺省动作，即对未匹配ACL的报文所采取的动作，Deny表示拒绝通过。如缺省过滤动作为允许通过，则不显示该字段。 |

### 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以及报文过滤缺省动作的统计信息。

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

**global**：显示全局（即所有物理接口）统计信息。

**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。

**default**：显示报文过滤缺省动作的统计信息。

*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：若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL；否则表示 IPv6 基本 ACL。

- 3000～3999：若未指定 **ipv6** 关键字，表示 IPv4 高级 ACL；否则表示 IPv6 高级 ACL。
- 4000～4999：表示二层 ACL（指定 **ipv6** 关键字后不会显示本项）。

**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，必须以英文字母 a～z 或 A～Z 开头。对于基本 ACL 或高级 ACL，若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称，否则表示 IPv6 基本 ACL 或 IPv6 高级 ACL 的名称。

**brief**：显示简要统计信息。

【使用指导】

若未指定 **default**、*acl-number* 和 **name** *acl-name* 参数，将显示全部 ACL（若未指定 **ipv6** 关键字，表示全部 IPv4 基本 ACL、IPv4 高级 ACL 和二层 ACL；否则，表示全部 IPv6 基本 ACL 和 IPv6 高级 ACL）在报文过滤中应用的统计信息以及报文过滤缺省动作的统计信息。

【举例】

# 显示接口 GigabitEthernet3/0/1 入方向上全部 ACL（包括 IPv4 基本 ACL、IPv4 高级 ACL 和二层 ACL）在报文过滤中应用的统计信息。

```
<Sysname> display packet-filter statistics interface gigabitethernet 3/0/1 inbound
Interface: GigabitEthernet3/0/1
In-bound policy:
  ACL 2001, Hardware-count
   From 2012-11-16 09:07:29 to 2012-11-16 09:14:03
   rule 0 permit
   Totally 0 packets, 0% permitted
   Totally 0 packets, 0% denied

  Default action: Deny
```

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 |
| In-bound policy | 在入方向上应用的统计信息 |
| Out-bound policy | 在出方向上应用的统计信息 |
| ACL 2001 | IPv4基本ACL 2001应用成功 |
| Hardware-count | 规则匹配统计功能应用成功 |
| From 2012-11-16 09:07:29 to 2012-11-16 09:14:03 | 该统计的起始和终止时间 |
| Totally 0 packets, 0% permitted | 该ACL允许符合条件报文的个数和通过率 |
| Totally 0 packets, 0% denied | 该ACL拒绝符合条件报文的个数和丢弃率 |
| Default action | 报文过滤缺省动作，即对未匹配ACL的报文所采取的动作，Deny表示拒绝通过。如缺省过滤动作为允许通过，则不显示该字段 |

【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** ] { *acl-number* | **name** *acl-name* } [ **brief** ]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-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。

*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：若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL；否则表示 IPv6 基本 ACL。
- 3000～3999：若未指定 **ipv6** 关键字，表示 IPv4 高级 ACL；否则表示 IPv6 高级 ACL。
- 4000～4999：表示二层 ACL（指定 **ipv6** 关键字后不会显示本项）。

**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，必须以英文字母 a～z 或 A～Z 开头。对于基本 ACL 或高级 ACL，若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称，否则表示 IPv6 基本 ACL 或 IPv6 高级 ACL 的名称。

**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:
 In-bound policy:
  ACL 2001
   rule 0 permit source 2.2.2.2 0 (2 packets)
   rule 5 permit source 1.1.1.1 0
   rule 10 permit vpn-instance test
   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 |
| In-bound policy | ACL在入方向上应用的累加统计信息 |
| Out-bound policy | ACL在出方向上应用的累加统计信息 |
| 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, 100% permitted | 该ACL允许符合条件报文的个数和通过率 |
| Totally 0 packets, 0% denied | 该ACL拒绝符合条件报文的个数和丢弃率 |

【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** { **global** | **interface** *interface-type interface-number* } { **inbound** | **outbound** } [ [ **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

mdc-admin

mdc-operator

【参数】

**global**：显示 ACL 在报文过滤中的全局（即所有物理接口）详细应用情况。

**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。

**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。

*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：若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL；否则表示 IPv6 基本 ACL。
- 3000～3999：若未指定 **ipv6** 关键字，表示 IPv4 高级 ACL；否则表示 IPv6 高级 ACL。
- 4000～4999：表示二层 ACL（指定 **ipv6** 关键字后不会显示本项）。

**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，必须以英文字母 a～z 或 A～Z 开头。对于基本 ACL 或高级 ACL，若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称，否则表示 IPv6 基本 ACL 或 IPv6 高级 ACL 的名称。

**slot** *slot-number*：显示指定单板上 ACL 在报文过滤中的详细应用情况，*slot-number* 表示单板所在的槽位号。若未指定本参数，将显示主用主控板上 ACL 在报文过滤中的详细应用情况。

【使用指导】

若未指定 *acl-number* 和 **name** *acl-name* 参数，将显示全部 ACL（若未指定 **ipv6** 关键字，表示全部 IPv4 基本 ACL、IPv4 高级 ACL 和二层 ACL；否则，表示全部 IPv6 基本 ACL 和 IPv6 高级 ACL）在报文过滤中的详细应用情况。

【举例】

# 显示接口 GigabitEthernet3/0/1 入方向上全部 ACL（包括 IPv4 基本 ACL、IPv4 高级 ACL 和二层 ACL）在报文过滤中的详细应用情况。

```
<Sysname> display packet-filter verbose interface gigabitethernet 3/0/1 inbound
Interface: GigabitEthernet3/0/1
In-bound policy:
  ACL 2001, Hardware-count
   rule 0 permit source 2.2.2.2 0
   rule 5 permit source 1.1.1.1 0

  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 |
| In-bound policy | ACL在入方向上的详细应用情况 |
| Out-bound policy | ACL在出方向上的详细应用情况 |
| ACL 2001 | IPv4基本ACL 2001应用成功 |
| Hardware-count | 规则匹配统计功能应用成功 |
| Default action | 报文过滤缺省动作，即对未匹配ACL的报文所采取的动作，Deny表示拒绝通过。如缺省过滤动作为允许通过，则不显示该字段 |

## 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

mdc-admin

mdc-operator

【参数】

**slot** *slot-number*：显示指定单板上 QoS 和 ACL 资源的使用情况，*slot-number* 表示单板所在的槽位号。若未指定本参数，将显示所有单板上 QoS 和 ACL 资源的使用情况。

【举例】

# 显示 QoS 和 ACL 资源的使用情况。

```
<Sysname> display qos-acl resource
Interfaces: GE2/0/1 to GE2/0/24, XGE2/0/25 to XGE2/0/26
-------------------------------------------------------------------------
 Type             Total      Reserved   Configured Remaining  Usage
-------------------------------------------------------------------------
 IPv4Acl          65536      0          0          65536      0%
 IPv6Acl          16384      0          0          16384      0%
 Car&Cnt          32768      0          0          32768      0%
 InBRASCar        65536      0          5138       60398      7%
 OutBRASCar       65536      0          5142       60394      7%
 TCPCar           16384      0          5151       11233      31%
 CarProf          220        0          4          216        1%
 Sampler          32768      0          0          32768      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 |
| Total | 资源总数 |
| Reserved | 预留的资源数 |
| Configured | 已经配置的资源数 |
| Remaining | 剩余可用的资源数 |
| Usage | 已使用资源的百分比 |

## 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** ] { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** } [ **hardware-count** ]

**undo packet-filter** [ **ipv6** ] { *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

mdc-admin

【参数】

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

- 2000～2999：若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL；否则表示 IPv6 基本 ACL。
- 3000～3999：若未指定 **ipv6** 关键字，表示 IPv4 高级 ACL；否则表示 IPv6 高级 ACL。
- 4000～4999：表示二层 ACL（指定 **ipv6** 关键字后不会显示本项）。

**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。对于基本 ACL 或高级 ACL，若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称，否则表示 IPv6 基本 ACL 或 IPv6 高级 ACL 的名称。

**inbound**：对收到的报文进行过滤。

**outbound**：对发出的报文进行过滤。

**hardware-count**：表示使能规则匹配统计功能，缺省为关闭。本参数用于使能指定 ACL 内所有规则的匹配统计功能，而 **rule** 命令中的 **counting** 参数则用于使能当前规则的匹配统计功能。

【举例】

# 应用 IPv4 基本 ACL 2001 对接口 GigabitEthernet3/0/1 收到的报文进行过滤，并对过滤的报文进行统计。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] 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

mdc-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 packet-filter default hardware-count

**packet-filter default hardware-count** 命令用来在接口上使能报文过滤缺省动作统计功能。

**undo packet-filter default hardware-count** 命令用来在接口上关闭报文过滤缺省动作统计功能。

【命令】

**packet-filter default** { **inbound** | **outbound** } **hardware-count**

**undo packet-filter default** { **inbound** | **outbound** } **hardware-count**

【缺省情况】

报文过滤缺省动作统计功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

**inbound**：表示收到的报文。

**outbound**：表示发出的报文。

【使用指导】

在接口上只有应用了 ACL 进行报文过滤，才允许使能报文过滤缺省动作统计功能。

【举例】

# 配置报文过滤的缺省动作为 Deny，在接口 GigabitEthernet3/0/1 上对收到的报文应用 IPv4 基本 ACL 2001 进行过滤，并使能报文过滤缺省动作统计功能。

```
<Sysname> system-view
[Sysname] packet-filter default deny
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] packet-filter 2001 inbound
[Sysname-GigabitEthernet3/0/1] packet-filter default inbound hardware-count
```

【相关命令】

- **packet-filter**
- **packet-filter default deny**
- **display packet-filter**
- **display packet-filter statistics**

### 1.1.15 reset acl counter

**reset acl counter** 命令用来清除 ACL 的统计信息。

【命令】

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

【视图】

用户视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

*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：若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL；否则表示 IPv6 基本 ACL。
- 3000～3999：若未指定 **ipv6** 关键字，表示 IPv4 高级 ACL；否则表示 IPv6 高级 ACL。
- 4000～4999：表示二层 ACL（指定 **ipv6** 关键字后不会显示本项）。

**all**：清除全部 ACL 的统计信息。若未指定 **ipv6** 关键字，表示全部 IPv4 基本 ACL、IPv4 高级 ACL 和二层 ACL；否则，表示全部 IPv6 基本 ACL 和 IPv6 高级 ACL。

**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，必须以英文字母 a～z 或 A～Z 开头。对于基本 ACL 或高级 ACL，若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称，否则表示 IPv6 基本 ACL 或 IPv6 高级 ACL 的名称。

【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**

### 1.1.16 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（包括累加统计信息）。

【命令】

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

【视图】

用户视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

**global**：清除全局（即所有物理接口）统计信息。

**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。

*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：若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL；否则表示 IPv6 基本 ACL。
- 3000～3999：若未指定 **ipv6** 关键字，表示 IPv4 高级 ACL；否则表示 IPv6 高级 ACL。
- 4000～4999：表示二层 ACL（指定 **ipv6** 关键字后不会显示本项）。

**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，必须以英文字母 a～z 或 A～Z 开头。对于基本 ACL 或高级 ACL，若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称，否则表示 IPv6 基本 ACL 或 IPv6 高级 ACL 的名称。

【使用指导】

若未指定 **default**、*acl-number* 和 **name** *acl-name* 参数，将清除全部 ACL（若未指定 **ipv6** 关键字，表示全部 IPv4 基本 ACL、IPv4 高级 ACL 和二层 ACL；否则，表示全部 IPv6 基本 ACL 和 IPv6 高级 ACL）和缺省动作在报文过滤中应用的统计信息。

【举例】

# 清除接口 Ten-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 Ten-GigabitEthernet 3/0/1 inbound 2001
```

【相关命令】

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

### 1.1.17 rule (Ethernet frame header 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** *vlan-pri* | **counting** | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name* ] *

**undo rule** *rule-id* [ **counting** | **time-range** ] *

【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

mdc-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，系统将按照步长从 0 开始，自动分配一个大于现有最大编号的最小编号。譬如现有规则的最大编号为 28，步长为 5，那么自动分配的新编号将是 30。

**deny**：表示拒绝符合条件的报文。

**permit**：表示允许符合条件的报文。

**cos** *vlan-pri*：指定 802.1p 优先级。*vlan-pri* 表示 802.1p 优先级，可输入的形式如下：

- 数字：取值范围为 0～7；
- 名称：**best-effort**、**background**、**spare**、**excellent-effort**、**controlled-load**、**video**、**voice** 和 **network-management**，依次对应于数字 0～7。

**counting**：表示使能规则匹配统计功能，缺省为关闭。本参数用于使能本规则的匹配统计功能，而 **packet-filter** 命令中的 **hardware-count** 参数则用于使能指定 ACL 内所有规则的匹配统计功能。

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

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

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

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

**time-range** *time-range-name*：指定本规则生效的时间段。*time-range-name* 表示时间段的名称，为 1～32 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。若该时间段尚未配置，该规则仍会成功创建但系统将给出提示信息，并在该时间段的配置完成后此规则才会生效。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。
- 使用 **undo rule** 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- 使用 **undo rule** 命令时必须指定一个已存在规则的编号，可以使用 **display acl all** 命令来查看所有已存在的规则。

【举例】

# 为二层 ACL 4000 创建规则如下：允许 ARP 报文通过，但拒绝 RARP 报文通过。

```
<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] rule permit type 0806 ffff
[Sysname-acl-ethernetframe-4000] rule deny type 8035 ffff
```

【相关命令】

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

## 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** { *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* | **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** ] *

【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

mdc-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，系统将按照步长从 0 开始，自动分配一个大于现有最大编号的最小编号。譬如现有规则的最大编号为 28，步长为 5，那么自动分配的新编号将是 30。

**deny**：表示拒绝符合条件的报文。

**permit**：表示允许符合条件的报文。

*protocol*：表示 IPv4 承载的协议类型，可输入的形式如下：

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

*protocol*之后可配置如 表 1-7 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** { *source-address source-wildcard* \| **any** } | 源地址信息 | 指定ACL规则的源地址信息 | *source-address*：源IP地址<br>*source-wildcard*：源IP地址的通配符掩码（为0表示主机地址）<br>**any**：任意源IP地址 |
| **destination** { *dest-address dest-wildcard* \| **any** } | 目的地址信息 | 指定ACL规则的目的地址信息 | *dest-address*：目的IP地址<br>*dest-wildcard*：目的IP地址的通配符掩码（为0表示主机地址）<br>**any**：任意目的IP地址 |

| 参数 | 类别 | 作用 | 说明 |
| --- | --- | --- | --- |
| **counting** | 统计 | 使能规则匹配统计功能，缺省为关闭 | 本参数用于使能本规则的匹配统计功能，而**packet-filter**命令中的**hardware-count**参数则用于使能指定ACL内所有规则的匹配统计功能 |
| **precedence** *precedence* | 报文优先级 | IP优先级 | *precedence*用数字表示时，取值范围为0～7；用文字表示时，分别对应**routine**、**priority**、**immediate**、**flash**、**flash-override**、**critical**、**internet**、**network** |
| **tos** *tos* | 报文优先级 | ToS优先级 | *tos*用数字表示时，取值范围为0～15；用文字表示时，可以选取**max-reliability**（2）、**max-throughput**（4）、**min-delay**（8）、**min-monetary-cost**（1）、**normal**（0） |
| **dscp** *dscp* | 报文优先级 | DSCP优先级 | *dscp*用数字表示时，取值范围为0～63；用文字表示时，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<br>CSPC单板和丝印为CMPE-1104的单板不支持该参数 |
| **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** *time-range-name* | 时间段 | 指定本规则生效的时间段 | *time-range-name*：时间段的名称，为1～32个字符的字符串，不区分大小写，必须以英文字母a～z或A～Z开头。若该时间段尚未配置，该规则仍会成功创建但系统将给出提示信息，并在该时间段的配置完成后此规则才会生效。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<br>若未指定本参数，表示该规则仅对非VPN报文有效<br>CSPC单板和丝印为CMPE-1104的单板不支持该参数 |

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** *operator port1* [ *port2* ] | 源端口 | 定义TCP/UDP报文的源端口信息 | *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**需要两个端口号做操作数，其它的只需要一个端口号做操作数<br>*port1*、*port2*：TCP或UDP的端口号，用数字表示时，取值范围为0～65535；用文字表示时，TCP端口号可以选取**chargen**（19）、**bgp**（179）、**cmd**（514）、**daytime**（13）、**discard**（9）、**domain**（53）、**echo**（7）、**exec**（512）、**finger**（79）、**ftp**（21）、**ftp-data**（20）、**gopher**（70）、**hostname**（101）、**irc**（194）、**klogin**（543）、**kshell**（544）、**login**（513）、**lpd**（515）、**nntp**（119）、**pop2**（109）、**pop3**（110）、**smtp**（25）、**sunrpc**（111）、**tacacs**（49）、**talk**（517）、**telnet**（23）、**time**（37）、**uucp**（540）、**whois**（43）、**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） |
| **destination-port** *operator port1* [ *port2* ] | 目的端口 | 定义TCP/UDP报文的目的端口信息 | |
| { **ack** *ack-value* \| **fin** *fin-value* \| **psh** *psh-value* \| **rst** *rst-value* \| **syn** *syn-value* \| **urg** *urg-value* } * | TCP报文标识 | 定义对携带不同标志位（包括ACK、FIN、PSH、RST、SYN和URG六种）的TCP报文的处理规则 | TCP协议特有的参数。表示匹配携带不同标志位的TCP报文，各*value*的取值可为0或1（0表示不携带此标志位，1表示携带此标志位）<br>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，有些产品将匹配不携带ACK标志位且携带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** { *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<br>*icmp-code*：ICMP消息码，取值范围为0～255<br>*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1-10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。
- 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。
- 使用 **undo rule** 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- 使用 **undo rule** 命令时必须指定一个已存在规则的编号，可以使用 **display acl all** 命令来查看所有已存在的规则。
- CSPC 单板和丝印为 CMPE-1104 的单板不支持配置操作符 *operator* 取值为 **neq**。

【举例】

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

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

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

```
<Sysname> system-view
[Sysname] acl number 3001
[Sysname-acl-adv-3001] rule deny icmp destination 192.168.1.0 0.0.0.255
[Sysname-acl-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 number 3002
[Sysname-acl-adv-3002] rule permit tcp source-port eq ftp
[Sysname-acl-adv-3002] rule permit tcp source-port eq ftp-data
[Sysname-acl-adv-3002] rule permit tcp destination-port eq ftp
[Sysname-acl-adv-3002] rule permit tcp destination-port eq ftp-data
```

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

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

【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** { *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** ] *

【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

mdc-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，系统将按照步长从 0 开始，自动分配一个大于现有最大编号的最小编号。譬如现有规则的最大编号为 28，步长为 5，那么自动分配的新编号将是 30。

**deny**：表示拒绝符合条件的报文。

**permit**：表示允许符合条件的报文。

**counting**：表示使能规则匹配统计功能，缺省为关闭。本参数用于使能本规则的匹配统计功能，而 **packet-filter** 命令中的 **hardware-count** 参数则用于使能指定 ACL 内所有规则的匹配统计功能。

**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。CSPC 单板和丝印为 CMPE-1104 的单板不支持该参数。

**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”。

**vpn-instance** *vpn-instance-name*：表示对指定 VPN 实例中的报文有效。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。若未指定本参数，表示该规则仅对非 VPN 报文有效。SPC 单板和丝印为 MPE-1104 的单板不支持该参数。

【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。

- 使用 **undo rule** 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- 使用 **undo rule** 命令时必须指定一个已存在规则的编号，可以使用 **display acl all** 命令来查看所有已存在的规则。

【举例】

# 为 IPv4 基本 ACL 2000 创建规则如下：仅允许来自 10.0.0.0/8、172.17.0.0/16 和 192.168.1.0/24 网段的报文通过，而拒绝来自所有其它网段的报文通过。

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.0.0.0 0.255.255.255
[Sysname-acl-basic-2000] rule permit source 172.17.0.0 0.0.255.255
[Sysname-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Sysname-acl-basic-2000] rule deny source any
```

【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** { *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* | **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** ] *

【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

mdc-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，系统将按照步长从 0 开始，自动分配一个大于现有最大编号的最小编号。譬如现有规则的最大编号为 28，步长为 5，那么自动分配的新编号将是 30。

**deny**：表示拒绝符合条件的报文。

**permit**：表示允许符合条件的报文。

*protocol*：表示 IPv6 承载的协议类型，可输入的形式如下：

- 数字：取值范围为 0～255；
- 名称（括号内为对应的数字）：可选取 **gre**（47）、**icmpv6**（58）、**ipv6**、**ipv6-ah**（51）、**ipv6-esp**（50）、**ospf**（89）、**tcp**（6）或 **udp**（17）。

*protocol*之后可配置如 表 1-11 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** { *source-address source-prefix* \| *source-address/source-prefix* \| **any** } | 源IPv6地址 | 指定ACL规则的源IPv6地址信息 | *source-address*：源IPv6地址<br>*source-prefix*：源IPv6地址的前缀长度，取值范围1～128<br>**any**：任意源IPv6地址 |
| **destination** { *dest-address dest-prefix* \| *dest-address/dest-prefix* \| **any** } | 目的IPv6地址 | 指定ACL规则的目的IPv6地址信息 | *dest-address*：目的IPv6地址<br>*dest-prefix*：目的IPv6地址的前缀长度，取值范围1～128<br>**any**：任意目的IPv6地址 |
| **counting** | 统计 | 使能规则匹配统计功能，缺省为关闭 | 本参数用于使能本规则的匹配统计功能，而**packet-filter ipv6**命令中的**hardware-count**参数则用于使能指定ACL内所有规则的匹配统计功能 |
| **dscp** *dscp* | 报文优先级 | DSCP优先级 | *dscp*：用数字表示时，取值范围为0～63；用名称表示时，可选取**af11**（10）、**af12**（12）、**af13**（14）、**af21**（18）、**af22**（20）、**af23**（22）、**af31**（26）、**af32**（28）、**af33**（30）、**af41**（34）、**af42**（36）、**af43**（38）、**cs1**（8）、**cs2**（16）、**cs3**（24）、**cs4**（32）、**cs5**（40）、**cs6**（48）、**cs7**（56）、**default**（0）或**ef**（46） |
| **flow-label** *flow-label-value* | 流标签字段 | 指定IPv6基本报文头中流标签字段的值 | *flow-label-value*：流标签字段的值，取值范围为0～1048575 |

| 参数 | 类别 | 作用 | 说明 |
| --- | --- | --- | --- |
| **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<br>CSPC单板和丝印为CMPE-1104的单板不支持该参数 |
| **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** *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<br>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<br>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 |
| **time-range** *time-range-name* | 时间段 | 指定本规则生效的时间段 | *time-range-name*：时间段的名称，为1～32个字符的字符串，不区分大小写，必须以英文字母a～z或A～Z开头。若该时间段尚未配置，该规则仍会成功创建但系统将给出提示信息，并在该时间段的配置完成后此规则才会生效。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<br>若未指定本参数，表示该规则仅对非VPN报文有效<br>CSPC单板和丝印为CMPE-1104的单板不支持该参数 |

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** *operator port1* [ *port2* ] | 源端口 | 定义TCP/UDP报文的源端口信息 | *operator*：操作符，取值可以为**lt**（小于）、**gt**（大于）、**eq**（等于）、**neq**（不等于）或者**range**（在范围内，包括边界值）。只有**range**操作符需要两个端口号做操作数，其它操作符只需要一个端口号做操作数<br>*port1*/*port2*：TCP或UDP的端口号，用数字表示时，取值范围为0～65535；用名称表示时，TCP端口号可选取**chargen**（19）、**bgp**（179）、**cmd**（514）、**daytime**（13）、**discard**（9）、**domain**（53）、**echo**（7）、**exec**（512）、**finger**（79）、**ftp**（21）、**ftp-data**（20）、**gopher**（70）、**hostname**（101）、**irc**（194）、**klogin**（543）、**kshell**（544）、**login**（513）、**lpd**（515）、**nntp**（119）、**pop2**（109）、**pop3**（110）、**smtp**（25）、**sunrpc**（111）、**tacacs**（49）、**talk**（517）、**telnet**（23）、**time**（37）、**uucp**（540）、**whois**（43）或**www**（80）；UDP端口号可选取**biff**（512）、**bootpc**（68）、**bootps**（67）、**discard**（9）、**dns**（53）、**dnsix**（90）、**echo**（7）、**mobilip-ag**（434）、**mobilip-mn**（435）、**nameserver**（42）、**netbios-dgm**（138）、**netbios-ns**（137）、**netbios-ssn**（139）、**ntp**（123）、**rip**（520）、**snmp**（161）、**snmptrap**（162）、**sunrpc**（111）、**syslog**（514）、**tacacs-ds**（65）、**talk**（517）、**tftp**（69）、**time**（37）、**who**（513）或**xdmcp**（177） |
| **destination-port** *operator port1* [ *port2* ] | 目的端口 | 定义TCP/UDP报文的目的端口信息 | |
| { **ack** *ack-value* \| **fin** *fin-value* \| **psh** *psh-value* \| **rst** *rst-value* \| **syn** *syn-value* \| **urg** *urg-value* } * | TCP报文标识 | 定义对携带不同标志位（包括ACK、FIN、PSH、RST、SYN和URG六种）的TCP报文的处理规则 | TCP协议特有的参数。表示匹配携带不同标志位的TCP报文，各*value*的取值可为0或1（0表示不携带此标志位，1表示携带此标志位）<br>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，有些产品将匹配不携带ACK标志位且携带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** { *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<br>*icmp6-code*：ICMPv6消息码，取值范围为0～255<br>*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1-14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】

- 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。
- 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。
- 使用 **undo rule** 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- 使用 **undo rule** 命令时必须指定一个已存在规则的编号，可以使用 **display acl ipv6 all** 命令来查看所有已存在的规则。
- 如果 ACL 匹配的是 IPv6 扩展报文头内层的报文内容，则对于扩展报文头超过两层，或包含 Encapsulating Security Payload Header 报文头的报文，ACL 将无法进行匹配。
- CSPC 单板和丝印为 CMPE-1104 的单板不支持配置操作符 *operator* 取值为 **neq**。
- 需要注意的是，当 IPv6 高级 ACL 用于 QoS 策略的流分类或用于报文过滤功能时：如果 QoS 策略或报文过滤功能应用于出方向，不支持配置 **routing** 参数和 **flow-label** 参数。

【举例】

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

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

# 为 IPv6 高级 ACL 3001 创建规则如下：允许 IPv6 报文通过，但拒绝发往 FE80:5060:1001::/48 网段的 ICMPv6 报文通过。

```
<Sysname> system-view
[Sysname] acl ipv6 number 3001
[Sysname-acl6-adv-3001] rule deny icmpv6 destination fe80:5060:1001:: 48
[Sysname-acl6-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 number 3002
[Sysname-acl6-adv-3002] rule permit tcp source-port eq ftp
[Sysname-acl6-adv-3002] rule permit tcp source-port eq ftp-data
[Sysname-acl6-adv-3002] rule permit tcp destination-port eq ftp
[Sysname-acl6-adv-3002] rule permit tcp destination-port eq ftp-data
```

# 为 IPv6 高级 ACL 3003 创建规则如下：在出、入双方向上都允许 SNMP 报文和 SNMP Trap 报文通过。

```
<Sysname> system-view
[Sysname] acl ipv6 number 3003
[Sysname-acl6-adv-3003] rule permit udp source-port eq snmp
[Sysname-acl6-adv-3003] rule permit udp source-port eq snmptrap
[Sysname-acl6-adv-3003] rule permit udp destination-port eq snmp
[Sysname-acl6-adv-3003] rule permit udp destination-port eq snmptrap
```

# 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 number 3004
[Sysname-acl6-adv-3004] rule permit ipv6 hop-by-hop type 5
[Sysname-acl6-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** { *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** ] *

【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

mdc-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，系统将按照步长从 0 开始，自动分配一个大于现有最大编号的最小编号。譬如现有规则的最大编号为 28，步长为 5，那么自动分配的新编号将是 30。

**deny**：表示拒绝符合条件的报文。

**permit**：表示允许符合条件的报文。

**counting**：表示使能规则匹配统计功能，缺省为关闭。本参数用于使能本规则的匹配统计功能，而 **packet-filter ipv6** 命令中的 **hardware-count** 参数则用于使能指定 ACL 内所有规则的匹配统计功能。

**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。CSPC 单板和丝印为 CMPE-1104 的单板不支持该参数。

**logging**：表示对符合条件的报文可记录日志信息。该功能需要使用该 ACL 的模块支持日志记录功能，例如报文过滤。

**routing** [ **type** *routing-type* ]：表示对所有或指定类型的路由头有效，*routing-type* 表示路由头类型的值，取值范围为 0～255。若指定了 **type** *routing-type* 参数，表示仅对指定类型的路由头有效；否则，表示对所有类型的路由头都有效。

**source** { *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”。

**vpn-instance** *vpn-instance-name*：表示对指定 VPN 实例中的报文有效。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。若未指定本参数，表示该规则仅对非 VPN 报文有效。CSPC 单板和丝印为 CMPE-1104 的单板不支持该参数。

【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。
- 使用 **undo rule** 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- 使用 **undo rule** 命令时必须指定一个已存在规则的编号，可以使用 **display acl ipv6 all** 命令来查看所有已存在的规则。
- CSPC 单板和丝印为 CMPE-1104 的单板不支持 **fragment** 参数和 **vpn-instance** 参数。

【举例】

# 为 IPv6 基本 ACL 2000 创建规则如下：仅允许来自 1001::/16、3124:1123::/32 和 FE80:5060:1001::/48 网段的报文通过，而拒绝来自所有其它网段的报文通过。

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source 1001:: 16
[Sysname-acl6-basic-2000] rule permit source 3124:1123:: 32
[Sysname-acl6-basic-2000] rule permit source fe80:5060:1001:: 48
[Sysname-acl6-basic-2000] rule deny source any
```

【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 comment

**rule comment** 命令用来为指定规则配置描述信息。

**undo rule comment** 命令用来删除指定规则的描述信息。

【命令】

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

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

【缺省情况】

规则没有任何描述信息。

【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

mdc-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 number 2000
[Sysname-acl-basic-2000] rule 0 deny source 1.1.1.1 0
[Sysname-acl-basic-2000] rule 0 comment This rule is used on GigabitEthernet 3/0/1.
```

【相关命令】

- **display acl**

### 1.1.23 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。

【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

mdc-admin

【参数】

*step-value*：表示规则编号的步长值，取值范围为 1～20。

【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 number 2000
[Sysname-acl-basic-2000] step 2
```

【相关命令】

- **display acl**