目 录

1 ACL ····· 1-1

1.1 ACL配置命令 ····· 1-1

1.1.1 acl ····· 1-1

1.1.2 acl accelerate ····· 1-2

1.1.3 acl copy ····· 1-3

1.1.4 acl ipv6 ····· 1-4

1.1.5 acl ipv6 copy ····· 1-5

1.1.6 acl ipv6 name ····· 1-6

1.1.7 acl name ····· 1-6

1.1.8 description ····· 1-7

1.1.9 display acl ····· 1-7

1.1.10 display acl accelerate ····· 1-9

1.1.11 display acl ipv6 ····· 1-11

1.1.12 display acl resource ····· 1-13

1.1.13 display time-range ····· 1-15

1.1.14 reset acl counter ····· 1-16

1.1.15 reset acl ipv6 counter ····· 1-17

1.1.16 rule (Ethernet frame header ACL view) ····· 1-17

1.1.17 rule (IPv4 advanced ACL view) ····· 1-19

1.1.18 rule (IPv4 basic ACL view) ····· 1-23

1.1.19 rule (IPv6 advanced ACL view) ····· 1-25

1.1.20 rule (IPv6 basic ACL view) ····· 1-29

1.1.21 rule comment ····· 1-31

1.1.22 rule remark ····· 1-31

1.1.23 step ····· 1-33

1.1.24 time-range ····· 1-34

1 ACL

1.1 ACL配置命令

1.1.1 acl

【命令】

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

undo acl { **all** | **name** *acl-name* | **number** *acl-number* }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

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

- 2000～2999：表示 IPv4 基本 ACL；
- 3000～3999：表示 IPv4 高级 ACL；
- 4000～4999：表示 IPv4 二层 ACL。

name *acl-name*：指定 ACL 的名称。*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 all。

match-order { **auto** | **config** }：指定规则的匹配顺序，**auto** 表示按照自动排序（即“深度优先”原则）的顺序进行规则匹配，**config** 表示按照配置顺序进行规则匹配。缺省情况下，规则的匹配顺序为配置顺序。

all：指定所指定全部 ACL（包括 IPv4 基本 ACL、IPv4 高级 ACL、二层 ACL）。

【描述】

acl 命令用来创建一个 IPv4 基本 ACL、IPv4 高级 ACL 或二层 ACL，并进入相应的 ACL 视图。**undo acl** 命令用来删除指定或全部 ACL（包括 IPv4 基本 ACL、IPv4 高级 ACL 和二层 ACL）。

缺省情况下，不存在任何 ACL。

需要注意的是：

- 使用 **acl** 命令时，如果指定编号的 ACL 不存在，则创建该 ACL 并进入其视图，否则直接进入其视图。
- ACL 的名称只能在创建时设置。ACL 一旦创建，便不允许再修改或删除原有名称。
- 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。
- 二层 ACL 仅支持对上送设备控制平面的以太网报文（如 VTY，local user）进行匹配，而转发平面的报文（如 QOS，firewall，debug 业务）无法通过二层 ACL 进行匹配。

相关配置可参考命令 **display acl**。

【举例】

创建一个编号为 2000 的 IPv4 基本 ACL，并进入其视图。

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

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

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

1.1.2 acl accelerate

【命令】

acl accelerate number *acl-number*

undo acl accelerate number *acl-number*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

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

- 2000～2999：表示 IPv4 基本 ACL；
- 3000～3999：表示 IPv4 高级 ACL。

【描述】

acl accelerate 命令用来使能指定 IPv4 基本 ACL 或 IPv4 高级 ACL 的加速功能。**undo acl accelerate** 命令用来关闭指定 IPv4 基本 ACL 或 IPv4 高级 ACL 的加速功能。

缺省情况下，所有 ACL 的加速功能均处于关闭状态。

需要注意的是：

- 只有当某 ACL 内有大量规则时，才有必要使能该 ACL 的加速功能。
- 如果某 ACL 内的规则中配置有不连续的通配符掩码（如 0.255.0.255），则不允许使能该 ACL 的加速功能。
- 由于加速功能会占用系统内存，因此只有当 ACL 内的规则达到一定数量时时，系统才允许使能该 ACL 的加速功能。否则，匹配速度不会得到明显提升，反而会占用大量内存。
- 如果使能了 ACL 的加速功能后又修改了该 ACL 的配置，加速功能仍将按照修改前的配置进行报文匹配。在这种情况下，建议先关闭再重新使能该 ACL 的加速功能，以保证报文能够正确匹配。

相关配置可参考命令 **display acl accelerate**。

【举例】

使能 IPv4 高级 ACL 3000 的加速功能。

```
<Sysname> system-view
[Sysname] acl accelerate number 3000
```

1.1.3 acl copy

【命令】

acl copy { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

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

- 2000～2999：表示 IPv4 基本 ACL；
- 3000～3999：表示 IPv4 高级 ACL；
- 4000～4999：表示 IPv4 二层 ACL。

name *source-acl-name*：指定源 ACL 的名称，该 ACL 必须存在。*source-acl-name* 为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。

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

- 2000～2999：表示 IPv4 基本 ACL；
- 3000～3999：表示 IPv4 高级 ACL；
- 4000～4999：表示 IPv4 二层 ACL。

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

【描述】

acl copy 命令用来复制并生成新的 IPv4 基本 ACL、IPv4 高级 ACL 或二层 ACL。

需要注意的是：

- 目的 ACL 的类型要与源 ACL 的类型相同。
- 目的 ACL 的名称只能在复制时设置。目的 ACL 一旦生成，便不允许再修改或删除其原有名称。
- 除了 ACL 的编号和名称不同外，新生成的 ACL（即目的 ACL）的匹配顺序、规则匹配统计功能的使能情况、规则编号的步长、所包含的规则、规则的描述信息以及 ACL 的描述信息等都与源 IPv4 ACL 的相同。

【举例】

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

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

1.1.4 acl ipv6

【命令】

acl ipv6 number *acl6-number* [**name** *acl6-name*] [**match-order** { **auto** | **config** }]

undo acl ipv6 { **all** | **name** *acl6-name* | **number** *acl6-number* }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

number *acl6-number*：指定 ACL 的编号。*acl6-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 IPv6 基本 ACL；
- 3000～3999：表示 IPv6 高级 ACL。

name *acl6-name*：指定 ACL 的名称。*acl6-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：指定全部 ACL（包括 IPv6 基本 ACL 和 IPv6 高级 ACL）。

【描述】

acl ipv6 命令用来创建一个 IPv6 基本 ACL 或 IPv6 高级 ACL，并进入相应的 ACL 视图。**undo acl ipv6** 命令用来删除指定或全部 ACL（包括 IPv6 基本 ACL 和 IPv6 高级 ACL）。

缺省情况下，不存在任何 ACL。

需要注意的是：

- 使用 **acl ipv6** 命令时，如果指定编号的 ACL 不存在，则创建该 ACL 并进入其视图，否则直接进入其视图。
- ACL 的名称只能在创建时设置。ACL 一旦创建，便不允许再修改或删除其原有名称。
- 当 ACL 内不存在任何规则时，用户可以使用本命令对该 ACL 的规则匹配顺序进行修改，否则不允许进行修改。

相关配置可参考命令 **display acl ipv6**。

【举例】

创建一个编号为 2000 的 IPv6 基本 ACL，并进入其视图。

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

创建一个编号为 2001 的 IPv6 基本 ACL，指定其名称为 flow，并进入其视图。

```
<Sysname> system-view
[Sysname] acl ipv6 number 2001 name flow
[Sysname-acl6-basic-2001-flow]
```

1.1.5 acl ipv6 copy

【命令】

acl ipv6 copy { *source-acl6-number* | **name** *source-acl6-name* } **to** { *dest-acl6-number* | **name** *dest-acl6-name* }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

source-acl6-number：指定源 ACL 的编号，该 ACL 必须存在。本参数的取值范围及其代表的 ACL 类型如下：

- 2000～2999：表示 IPv6 基本 ACL；
- 3000～3999：表示 IPv6 高级 ACL。

name *source-acl6-name*：指定源 ACL 的名称，该 ACL 必须存在。*source-acl6-name* 为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。

dest-acl6-number：指定目的 ACL 的编号，该 ACL 必须不存在。若未指定本参数，系统将为目的 ACL 自动分配一个与源 ACL 类型相同且可用的最小编号。本参数的取值范围及其代表的 ACL 类型如下：

- 2000～2999：表示 IPv6 基本 ACL；
- 3000～3999：表示 IPv6 高级 ACL。

name *dest-acl6-name*：指定目的 ACL 的名称，该 ACL 必须不存在。*dest-acl6-name* 为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 all。若未指定本参数，系统将不会为目的 ACL 设置名称。

【描述】

acl ipv6 copy 命令用来复制并生成新的 IPv6 基本 ACL 或 IPv6 高级 ACL。

需要注意的是：

- 目的 ACL 的类型要与源 ACL 的类型相同。
- 目的 ACL 的名称只能在复制时设置。目的 ACL 一旦生成，便不允许再修改或删除其原有名称。
- 除了 ACL 的编号和名称不同外，新生成的目的 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 IPv6 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 ipv6 copy 2001 to 2002
```

1.1.6 acl ipv6 name

【命令】

acl ipv6 name *acl6-name*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

acl6-name：指定 IPv6 基本 ACL 或 IPv6 高级 ACL 的名称，该 ACL 必须存在。为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。

【描述】

acl ipv6 name 命令用来进入指定名称的 IPv6 基本 ACL 或 IPv6 高级 ACL 视图。

相关配置可参考命令 **acl ipv6**。

【举例】

进入名称为 flow 的 IPv6 基本 ACL 的视图。

```
<Sysname> system-view
[Sysname] acl ipv6 name flow
[Sysname-acl6-basic-2001-flow]
```

1.1.7 acl name

【命令】

acl name *acl-name*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

acl-name：指定 IPv4 基本 ACL、IPv4 高级 ACL 或二层 ACL 的名称，该 ACL 必须存在。本参数为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。

【描述】

acl name 命令用来进入指定名称的 IPv4 基本 ACL、IPv4 高级 ACL 或二层 ACL 视图。

相关配置可参考命令 **acl**。

【举例】

进入名称为 flow 的 IPv4 基本 ACL 的视图。

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

1.1.8 description

【命令】

description *text*

undo description

【视图】

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

【缺省级别】

2：系统级

【参数】

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

【描述】

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

缺省情况下，ACL 没有任何描述信息。

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

【举例】

为 IPv4 基本 ACL 2000 配置描述信息。

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

为 IPv6 基本 ACL 2000 配置描述信息。

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] description This is an IPv6 basic ACL.
```

1.1.9 display acl

【命令】

非 IRF 模式：

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

IRF 模式：

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

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

acl-number：显示指定编号的 ACL 的配置和运行情况。*acl-number* 表示 IPv4 ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000～2999：表示 IPv4 基本 ACL；
- 3000～3999：表示 IPv4 高级 ACL；
- 4000～4999：表示二层 ACL。

all：显示全部 ACL（包括 IPv4 基本 ACL、IPv4 高级 ACL 和二层 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，必须以英文字母 a～z 或 A～Z 开头。

slot *slot-number*：显示指定单板上 ACL 的运行情况，*slot-number* 表示单板所在的槽位号。若未指定本参数，将显示设备整体的 ACL 配置情况。（非 IRF 模式）

SR6600/SR6600-X 路由器各款型对于本节所描述的参数的支持情况有所不同，详细差异信息如下：

型号	参数	描述
SR6602	**slot** *slot-number*	不支持
SR6602-X		支持
SR6604/SR6608/SR6616		支持
SR6604-X/SR6608-X/SR6616-X		支持

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备上指定单板的 ACL 运行情况，*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。若未指定本参数，将显示 IRF 设备整体的 ACL 配置情况。（IRF 模式）

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

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

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

【描述】

display acl 命令用来显示指定或全部 ACL（IPv4 基本 ACL、IPv4 高级 ACL 和二层 ACL）的配置和运行情况。

需要注意的是，本命令将按照实际匹配顺序来排列 ACL 内的规则，即：当 ACL 的规则匹配顺序为配置顺序时，各规则将按照编号由小到大排列；当 ACL 的规则匹配顺序为自动排序时，各规则将按照“深度优先”原则由深到浅排列。

【举例】

显示全部 ACL（包括 IPv4 基本 ACL、IPv4 高级 ACL 和二层 ACL）的配置和运行情况。

```
<Sysname> display acl all
Basic ACL  2000, named flow, 3 rules,
This is an IPv4 basic ACL.
ACL's step is 5
 rule 0 permit
 rule 5 permit source 1.1.1.1 0 (2 times matched)
 rule 10 permit vpn-instance mk

Basic ACL  2001, named -none-, 3 rules, match-order is auto,
ACL's step is 5
 rule 10 permit vpn-instance rd
 rule 10 comment This rule is used in VPN rd.
 rule 5 permit source 2.2.2.2 0
 rule 0 permit
```

表1-1 display acl 命令显示信息描述表

字段	描述
Basic ACL 2000	该ACL的类型和编号，ACL的类型包括： • Basic ACL：表示 IPv4 基本 ACL • Advanced ACL：表示 IPv4 高级 ACL • Ethernet frame ACL：表示 IPv4 二层 ACL
named flow	该ACL的名称为flow，-none-表示没有名称
3 rules	该ACL内包含的规则数量
match-order is auto	该ACL的规则匹配顺序为自动排序（匹配顺序为配置顺序时不显示本字段）
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
rule 0 permit	规则0的具体内容
2 times matched	该规则匹配的次数为2（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）
Uncompleted	该规则下发未完成，因此不会生效。这种情况通常是在ACL被动态修改之后，由于该规则的资源不足或硬件限制而导致其应用失败
rule 10 comment This rule is used in VPN rd.	规则10的描述信息

1.1.10 display acl accelerate

【命令】

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

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

acl-number：显示指定编号的 ACL 的加速功能相关信息。*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 IPv4 基本 ACL；
- 3000～3999：表示 IPv4 高级 ACL。

all：显示全部 ACL（包括 IPv4 基本 ACL 和 IPv4 高级 ACL）的加速功能相关信息。

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

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

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

【描述】

display acl accelerate 命令用来显示指定或全部 ACL（包括 IPv4 基本 ACL 和 IPv4 高级 ACL）加速功能的相关信息。

【举例】

显示指定或全部 ACL（包括 IPv4 基本 ACL 和 IPv4 高级 ACL）的加速功能相关信息。

```
<Sysname> display acl accelerate all
 Status: UTD -- up to date,  OOD -- out of date
 Accelerate: ACC -- accelerated,  UNACC -- unaccelerated

 Group            Accelerate           Status
 -------------------------------------------------
 2000             ACC                  UTD
 3000             ACC                  OOD
 3001             ACC                  UTD
 3002             UNACC                UTD
```

表1-2 display acl accelerate 命令显示信息描述表

字段	描述
Group	ACL的编号
Accelerate	ACL的加速标志： • ACC：表示该 ACL 已加速 • UNACC：表示该 ACL 未加速

字段	描述
Status	ACL加速快速查找库的状态信息： • UTD：表示该 ACL 的快速查找库信息已生效 • OOD：表示该 ACL 的快速查找库信息已失效 如果配置了ACL后再使能其加速功能，本字段将显示为UTD；如果使能了ACL的加速功能后又修改了该ACL的配置，本字段将显示为OOD，且加速功能仍将按照修改前的配置进行报文匹配，在这种情况下，建议先关闭再重新使能该ACL的加速功能，以保证报文能够正确匹配

1.1.11 display acl ipv6

【命令】

非 IRF 模式：

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

IRF 模式：

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

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

acl6-number：显示指定编号的 ACL 的配置和运行情况。*acl6-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 IPv6 基本 ACL；
- 3000～3999：表示 IPv6 高级 ACL。

all：显示所全部 ACL（包括 IPv6 基本 ACL 和 IPv6 高级 ACL）的配置和运行情况。

name *acl6-name*：显示指定名称的 ACL 的配置和运行情况。*acl6-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。

slot *slot-number*：显示指定单板上 ACL 的运行情况，*slot-number* 表示单板所在的槽位号。若未指定本参数，将显示设备整体的 ACL 配置情况。（非 IRF 模式）

SR6600/SR6600-X 路由器各款型对于本节所描述的参数的支持情况有所不同，详细差异信息如下：

型号	参数	描述
SR6602	**slot** *slot-number*	不支持
SR6602-X		支持
SR6604/SR6608/SR6616		支持
SR6604-X/SR6608-X/SR6616-X		支持

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备上指定单板的 ACL 运行情况，*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。若未指定本参数，将显示 IRF 设备整体的 ACL 配置情况。（IRF 模式）

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

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

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

【描述】

display acl ipv6 命令用来显示指定或全部 ACL（包括 IPv6 基本 ACL 和 IPv6 高级 ACL）的配置和运行情况。

需要注意的是，本命令将按照实际匹配顺序来排列 ACL 内的规则，即：当 ACL 的规则匹配顺序为配置顺序时，各规则将按照编号由小到大排列；当 ACL 的规则匹配顺序为自动排序时，各规则将按照“深度优先”原则由深到浅排列。

【举例】

显示指定或全部 ACL（包括 IPv6 基本 ACL 和 IPv6 高级 ACL）的配置和运行情况。

```
<Sysname> display acl ipv6 all
 Basic IPv6 ACL  2000, named flow, 3 rules,
 This is an IPv6 basic ACL.
 ACL's step is 5
 rule 0 permit
 rule 5 permit source 1::/64 (2 times matched)
 rule 10 permit vpn-instance mk

 Basic IPv6 ACL  2001, named -none-, 3 rules, match-order is auto,
 ACL's step is 5
 rule 10 permit vpn-instance rd
 rule 10 comment This rule is in VPN rd.
 rule 5 permit source 1::/64
 rule 0 permit
```

表1-3 display acl ipv6 命令显示信息描述表

字段	描述
Basic IPv6 ACL 2000	该ACL的类型和编号，ACL的类型包括： • Basic IPv6 ACL：表示 IPv6 基本 ACL • Advanced IPv6 ACL：表示 IPv6 高级 ACL
named flow	该ACL的名称为flow，-none-表示没有名称
3 rules	该ACL内包含的规则数量
This is an IPv6 basic ACL.	该ACL的描述信息
match-order is auto	该ACL的规则匹配顺序为自动排序（匹配顺序为配置顺序时不显示本字段）

字段	描述
ACL's step is 5	该ACL的规则编号的步长值为5
rule 0 permit	规则0的具体内容
2 times matched	该规则匹配的次数为2（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）
Uncompleted	该规则下发未完成，因此不会生效。这种情况通常是在ACL被动态修改之后，由于该规则的资源不足或硬件限制而导致其应用失败
rule 10 comment This rule is used in VPN rd.	规则10的描述信息.

1.1.12 display acl resource

【命令】

非 IRF 模式：

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

IRF 模式：

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

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

slot *slot-number*：显示指定单板上 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 ACL 资源的使用情况。（非 IRF 模式）

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备的指定单板上 ACL 资源的使用情况，*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。若未指定本参数，将显示 IRF 中所有成员设备的所有单板上 ACL 资源的使用情况。（IRF 模式）

【描述】

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

需要注意的是，如果指定的单板不支持统计 ACL 资源，则将只显示该单板的槽位号，而不会显示该单板上 ACL 资源的使用情况。

SR6600/SR6600-X 路由器各款型对于本节所描述的命令的支持情况有所不同，详细差异信息如下：

型号	命令	描述
SR6602	**display acl resource**	不支持
SR6602-X		不支持

型号	命令	描述
SR6604/SR6608/SR6616		配置了RPE-X1或RSE-X1主控板支持 配置了MCP主控板不支持
SR6604-X/SR6608-X/SR6616-X		支持

【举例】

显示设备 7 号槽位单板上 ACL 资源的使用情况。

```
<Sysname> display acl resource slot 7
Interface:
    GE7/0/0 to GE7/0/23
-------------------------------------------------------------------------------
  Type       Total   Reserved  Configured  Remaining
-------------------------------------------------------------------------------
 VFP ACL     1024     0         24          1000
 IFP ACL     4096     0         87          4009
 IFP Meter   2048     0         31          2017
 IFP Counter 2048     0         31          2017
 EFP ACL     512      0         0           512
 EFP Meter   256      0         0           256
 EFP Counter 512      0         0           512
 Interface:
    GE7/0/24 to GE7/0/47
-------------------------------------------------------------------------------
  Type       Total   Reserved  Configured  Remaining
-------------------------------------------------------------------------------
 VFP ACL     1024     0         24          1000
 IFP ACL     4096     0         87          4009
 IFP Meter   2048     0         31          2017
 IFP Counter 2048     0         31          2017
 EFP ACL     512      0         0           512
 EFP Meter   256      0         0           256
 EFP Counter 512      0         0           512
```

表1-4 display acl resource 命令显示信息描述表

字段	描述
Interface	接口名称，有接口类型和接口编号结合在一起组成
Type	资源类型： • ACL 表示 ACL 规则资源 • Meter 表示流量监管资源 • Counter 表示流量统计资源 • IFP 表示入方向的资源数目 • EFP 表示出方向的资源数目 • VFP 表示二层转发前的，应用于 QinQ 功能的资源数目

字段	描述
Total	支持的ACL规则总数
Reserved	预留的ACL规则数
Configured	已经配置的ACL规则数
Remaining	剩余的ACL规则数
VFP ACL	二层转发前的、应用于QinQ功能的ACL规则资源
IFP ACL	入方向的ACL规则资源
IFP Meter	入方向的流量监管资源
IFP Counter	入方向的流量统计资源
EFP ACL	出方向的ACL规则资源
EFP Meter	出方向的流量监管资源
EFP Counter	出方向的流量统计资源

1.1.13 display time-range

【命令】

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

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

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

all：显示所有时间段的配置和状态信息。

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

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

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

【描述】

display time-range 命令用来显示时间段的配置和状态信息。

【举例】

显示时间段 t4 的配置和状态信息。

```
<Sysname> display time-range t4
Current time is 17:12:34 4/13/2010 Tuesday

Time-range : t4 ( Inactive )
 10:00 to 12:00 Mon
 14:00 to 16:00 Wed
 from 00:00 1/1/2010 to 00:00 2/1/2010
 from 00:00 6/1/2010 to 00:00 7/1/2010
```

表1-5 display time-range 命令显示信息描述表

字段	描述
Current time	系统当前的时间
Time-range	时间段的配置信息，包括： • 时间段的名称 • 时间段的状态，包括 Active（生效）和 Inactive（未生效）两种状态 • 时间段的时间范围

1.1.14 reset acl counter

【命令】

reset acl counter { *acl-number* | **all** | **name** *acl-name* }

【视图】

用户视图

【缺省级别】

2：系统级

【参数】

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

- 2000～2999：表示 IPv4 基本 ACL；
- 3000～3999：表示 IPv4 高级 ACL；
- 4000～4999：表示 IPv4 二层 ACL。

all：指定全部 ACL（包括 IPv4 基本 ACL、IPv4 高级 ACL 和二层 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。

【描述】

reset acl counter 命令用来清除指定或全部 ACL（包括 IPv4 基本 ACL、IPv4 高级 ACL 和二层 ACL）的统计信息。

相关配置可参考命令 **display acl**。

【举例】

清除编号为 2001 的 IPv4 基本 ACL 的统计信息。

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

1.1.15 reset acl ipv6 counter

【命令】

reset acl ipv6 counter { *acl6-number* | **all** | **name** *acl6-name* }

【视图】

用户视图

【缺省级别】

2：系统级

【参数】

acl6-number：指定 ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000～2999：表示 IPv6 基本 ACL；
- 3000～3999：表示 IPv6 高级 ACL。

all：指定全部 ACL（包括 IPv6 基本 ACL 和 IPv6 高级 ACL）。

name *acl6-name*：指定 ACL 的名称。*acl6-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。

【描述】

reset acl ipv6 counter 命令用来清除指定或全部 ACL（包括 IPv6 基本 ACL 和 IPv6 高级 ACL）的统计信息。

相关配置可参考命令 **display acl ipv6**。

【举例】

清除编号为 2001 的 IPv6 基本 ACL 的统计信息。

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

1.1.16 rule (Ethernet frame header ACL view)

【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**] *

【视图】

二层 ACL 视图

【缺省级别】

2：系统级

【参数】

rule-id：指定二层 ACL 规则的编号，取值范围为 0～65534。若未指定本参数，系统将按照步长从 0 开始，自动分配一个大于现有最大编号的最小编号。譬如现有规则的最大编号为 28，步长为 5，那么自动分配的新编号将是 30。

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

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

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

counting：表示使能本规则的匹配统计功能，缺省为关闭。

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

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

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

source-mac *soucer-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。

【描述】

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

缺省情况下，二层 ACL 内不存在任何规则。

需要注意的是：

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

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

【举例】

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

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

1.1.17 rule (IPv4 advanced ACL view)

【命令】

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

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

【视图】

IPv4 高级 ACL 视图

【缺省级别】

2：系统级

【参数】

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

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

protocol：表示 IPv4 承载的协议类型，可输入的形式如下：

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

*protocol*之后可配置如 表 1-6 所示的规则信息参数。

表1-6 规则信息参数

参数	类别	作用	说明
source { *source-address sour-wildcard* | **any** }	源地址	指定ACL规则的源地址信息	*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

参数	类别	作用	说明
destination { *dest-address* *dest-wildcard* | **any** }	目的地址	指定ACL规则的目的地址信息	*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	使能本规则的匹配统计功能，缺省为关闭	-
precedence *precedence*	报文优先级	IP优先级	*precedence*：用数字表示时，取值范围为0～7；用名称表示时，为**routine**、**priority**、**immediate**、**flash**、**flash-override**、**critical**、**internet**或**network**，分别对应于数字0～7
tos *tos*	报文优先级	ToS优先级	*tos*：用数字表示时，取值范围为0～15；用名称表示时，可选取**max-reliability**（2）、**max-throughput**（4）、**min-delay**（8）、**min-monetary-cost**（1）或**normal**（0）
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）
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，例如防火墙
reflective	自反标志	设置规则具有自反属性	具有自反属性的ACL规则仅支持TCP、UDP、ICMP三种协议类型；动作类型只支持**permit**
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，表示该规则仅对非VPN报文有效
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报文无效	若未指定本参数，表示所有报文（包括非分片报文和分片报文的每个分片）均有效
time-range *time-range-name*	时间段信息	指定规则生效的时间段	*time-range-name*：时间段的名称，为1～32个字符的字符串，不区分大小写，必须以英文字母a～z或A～Z开头。若该时间段尚未配置，该规则仍会成功创建但系统将给出提示信息，并在该时间段的配置完成后此规则才会生效

注意

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

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

表1-7 TCP/UDP 特有的规则信息参数

参数	类别	作用	说明
source-port *operator port1* [*port2*]	源端口	定义TCP/UDP报文的源端口信息	*operator*：操作符，取值可以为**lt**（小于）、**gt**（大于）、**eq**（等于）、**neq**（不等于）或者**range**（在范围内，包括边界值）。只有**range**操作符需要两个端口号做操作数，其它操作符只需要一个端口号做操作数
destination-port *operator port1* [*port2*]	目的端口	定义TCP/UDP报文的目的端口信息	*port1*/*port2*：TCP或UDP的端口号，用数字表示时，取值范围为0～65535；用名称表示时，TCP端口号可选取**chargen**（19）、**bgp**（179）、**cmd**（514）、**daytime**（13）、**discard**（9）、**dns**（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）
{ **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）
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	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
host-redirect	5	1
host-tos-redirect	5	3
host-unreachable	3	1
information-reply	16	0
information-request	15	0
net-redirect	5	0
net-tos-redirect	5	2
net-unreachable	3	0
parameter-problem	12	0
port-unreachable	3	3
protocol-unreachable	3	2
reassembly-timeout	11	1
source-quench	4	0
source-route-failed	3	5
timestamp-reply	14	0
timestamp-request	13	0
ttl-exceeded	11	0

【描述】

rule 命令用来为 IPv4 高级 ACL 创建一条规则。**undo rule** 命令用来为 IPv4 高级 ACL 删除一条规则或删除规则中的部分内容。

缺省情况下，IPv4 高级 ACL 内不存在任何规则。

需要注意的是：

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

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

【举例】

为 IPv4 高级 ACL 3000 创建规则如下：允许 129.9.0.0/16 网段内的主机与 202.38.160.0/24 网段内主机的 WWW 端口（端口号为 80）建立连接，并对符合此条件的行为记录日志。

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

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

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

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

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

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

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

1.1.18 rule (IPv4 basic ACL view)

【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**] *

【视图】

IPv4 基本 ACL 视图

【缺省级别】

2：系统级

【参数】

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

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

counting：表示使能本规则的匹配统计功能，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，例如防火墙。

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

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

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

【描述】

rule 命令用来为 IPv4 基本 ACL 创建一条规则。**undo rule** 命令用来为 IPv4 基本 ACL 删除一条规则或删除规则中的部分内容。

缺省情况下，IPv4 基本 ACL 内不存在任何规则。

需要注意的是：

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

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

【举例】

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

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

1.1.19 rule (IPv6 advanced ACL view)

【命令】

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-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*] | **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** | **source** | **source-port** | **time-range** | **vpn-instance**] *

【视图】

IPv6 高级 ACL 视图

【缺省级别】

2：系统级

【参数】

rule-id：指定 IPv6 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 1-10 所示的规则信息参数。

表1-10 规则信息参数

参数	类别	作用	说明
source { *source-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 *source-prefix*：源IPv6地址的前缀长度，取值范围1～128 **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 *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	使能本规则的匹配统计功能，缺省为关闭	-
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
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，例如防火墙
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，表示对所有类型的路由头都有效
vpn-instance *vpn-instance-name*	VPN实例	对指定VPN实例中的报文有效	*vpn-instance-name*：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
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
time-range *time-range-name*	时间段	指定规则生效的时间段	*time-range-name*：时间段的名称，为1～32个字符的字符串，不区分大小写，必须以英文字母a～z或A～Z开头。若该时间段尚未配置，该规则仍会成功创建但系统将给出提示信息，并在该时间段的配置完成后此规则才会生效

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

表1-11 TCP/UDP 特有的规则信息参数

参数	类别	作用	说明
source-port *operator port1* [*port2*]	源端口	定义TCP/UDP报文的源端口信息	*operator*：操作符，取值可以为**lt**（小于）、**gt**（大于）、**eq**（等于）、**neq**（不等于）或者**range**（在范围内，包括边界值）。只有**range**操作符需要两个端口号做操作数，其它操作符只需要一个端口号做操作数 *port1*/*port2*：TCP或UDP的端口号，用数字表示时，取值范围为0～65535；用名称表示时，TCP端口号可选取**chargen**（19）、**bgp**（179）、**cmd**（514）、**daytime**（13）、**discard**（9）、**dns**（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）
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

ICMPv6 消息名称	ICMPv6 消息类型	ICMPv6 消息码
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

【描述】

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

缺省情况下，IPv6 高级 ACL 内不存在任何规则。

需要注意的是：

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

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

【举例】

为 IPv6 高级 ACL 3000 创建规则如下：允许 2030:5060::/64 网段内的主机与 FE80:5060::/96 网段内主机的 WWW 端口（端口号为 80）建立连接，并对符合此条件的行为记录日志。

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

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

```
<Sysname> system-view
[Sysname] acl ipv6 number 3001
[Sysname-acl6-adv-3001] rule permit ipv6
[Sysname-acl6-adv-3001] rule deny icmpv6 destination fe80:5060:1001:: 48
```

为 IPv6 高级 ACL 3002 创建规则如下：在出、入双方向上都允许建立 FTP 连接并传输 FTP 数据。

```
<Sysname> system-view
[Sysname] acl ipv6 number 3002
[Sysname-acl6-adv-3002] rule permit tcp source-port eq ftp
[Sysname-acl6-adv-3002] rule permit tcp source-port eq ftp-data
[Sysname-acl6-adv-3002] rule permit tcp destination-port eq ftp
[Sysname-acl6-adv-3002] rule permit tcp destination-port eq ftp-data
```

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

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

1.1.20 rule (IPv6 basic ACL view)

【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**] *

【视图】

IPv6 基本 ACL 视图

【缺省级别】

2：系统级

【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：表示使能本规则的匹配统计功能，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，例如防火墙。

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 地址前缀长度，取值范围为 1～128，**any** 表示任意源 IPv6 地址。

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

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

【描述】

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

缺省情况下，IPv6 基本 ACL 内不存在任何规则。

需要注意的是：

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

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

【举例】

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

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

```
[Sysname-acl6-basic-2000] rule permit source fe80:5060:1001:: 48
[Sysname-acl6-basic-2000] rule deny source any
```

1.1.21 rule comment

【命令】

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

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

【视图】

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

【缺省级别】

2：系统级

【参数】

rule-id：指定规则的编号，该规则必须存在。取值范围为 0～65534。

text：表示规则的描述信息，为 1～127 个字符的字符串，区分大小写。

【描述】

rule comment 命令用来为指定规则配置描述信息。**undo rule comment** 命令用来删除指定规则的描述信息。

缺省情况下，规则没有任何描述信息。

需要注意的是，使用 **rule comment** 命令时，如果指定的规则没有描述信息，则为其添加描述信息，否则修改其描述信息。

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

【举例】

为 IPv4 基本 ACL 2000 配置规则 0，并为该规则配置描述信息。

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule 0 deny source 1.1.1.1 0
[Sysname-acl-basic-2000] rule 0 comment This rule is used on GigabitEthernet 0/0.1.
```

为 IPv6 基本 ACL 2000 配置规则 0，并为该规则配置描述信息。

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule 0 permit source 1001::1 128
[Sysname-acl6-basic-2000] rule 0 comment This rule is used on GigabitEthernet 0/0.1.
```

1.1.22 rule remark

【命令】

rule [*rule-id*] **remark** *text*

undo rule [*rule-id*] **remark** [*text*]

【视图】

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

【缺省级别】

2：系统级

【参数】

rule-id：指定规则的编号（该编号对应的规则可以存在也可以不存在），取值范围为 0～65534。该编号用来确定规则注释信息显示的位置：

- 在配置顺序下：若该编号与现有某规则的编号相同，则该注释信息将紧邻该规则之前显示；否则，将按照编号由小到大显示。
- 在自动排序下：若该编号与现有某规则的编号相同，则该注释信息将紧邻该规则之前显示；否则，将在所有规则的最后显示。

【描述】

rule remark 命令用来配置规则注释信息。**undo rule remark** 命令用来删除规则注释信息。

缺省情况下，ACL 内没有任何规则注释信息。

需要注意的是：

- 使用 **rule remark** 命令时，如果没有指定 *rule-id* 参数，系统将按照步长从 0 开始，自动分配一个大于现有最大编号的最小编号。
- 使用 **undo rule remark** 命令时，如果没有指定 *rule-id* 和 *text* 参数，将删除所有规则注释信息；如果没有指定 *rule-id* 但指定了 *text* 参数，则只删除指定内容的规则注释信息。
- 用户可以通过 **display this** 和 **display current-configuration** 命令查看配置好的规则注释信息。

相关配置可参考“基础配置命令参考/配置文件管理”中的命令 **display this** 和 **display current-configuration**。

【举例】

在 IPv4 基本 ACL 2000 的视图下显示当前生效的配置信息，查看已有的规则。

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] display this
#
acl number 2000
 rule 0 permit source 14.1.1.0 0.0.0.255
 rule 5 permit source 10.1.1.1 0 time-range work-time
 rule 10 permit source 192.168.0.0 0.0.0.255
 rule 15 permit source 1.1.1.1 0
 rule 20 permit source 10.1.1.1 0
 rule 25 permit counting
#
return
```

假设规则编号为 10～25 的这四条规则是为 VIP 用户制订的，为方便后续维护，对这四条规则进行如下注释：开头和结尾分别注释为“Rules for VIP_start”和“Rules for VIP_end”。

```
[Sysname-acl-basic-2000] rule 10 remark Rules for VIP_start
[Sysname-acl-basic-2000] rule 26 remark Rules for VIP_end
```

再次在该 ACL 的视图下显示当前生效的配置信息，查看所配置的规则注释信息。

```
[Sysname-acl-basic-2000] display this
#
acl number 2000
 rule 0 permit source 14.1.1.0 0.0.0.255
 rule 5 permit source 10.1.1.1 0 time-range work-time
 rule 10 remark Rules for VIP_start
 rule 10 permit source 192.168.0.0 0.0.0.255
 rule 15 permit source 1.1.1.1 0
 rule 20 permit source 10.1.1.1 0
 rule 25 permit counting
 rule 26 remark Rules for VIP_end
#
return
```

由此可见，在规则编号为 10～25 的这四条规则的前、后均已插入了相应的注释信息。

1.1.23 step

【命令】

step *step-value*

undo step

【视图】

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

【缺省级别】

2：系统级

【参数】

step-value：表示规则编号的步长值，取值范围为 1～20。

【描述】

step 命令用来配置规则编号的步长。**undo step** 命令用来恢复缺省情况。

缺省情况下，规则编号的步长为 5。

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

【举例】

将基本 ACL 2000 的规则编号的步长配置为 2。

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

将 IPv6 基本 ACL 2000 的规则编号的步长配置为 2。

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] step 2
```

1.1.24 time-range

【命令】

time-range *time-range-name* { *start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* }

undo time-range *time-range-name* [*start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2*]

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

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

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

to *time2 date2*：指定绝对时间段的结束时间。*time2* 的格式为 hh:mm，hh 的取值范围为 00:00～24:00，mm 的取值范围为 0～59。*date2* 的格式为 MM/DD/YYYY 或 YYYY/MM/DD。MM 表示月，取值范围为 1～12；DD 表示日，取值范围取决于所输入的月份；YYYY 表示年，取值范围为 1970～2100。结束时间必须大于起始时间。若未指定本参数，绝对时间段的结束时间将为系统可表示的最晚时间，即 2100 年 12 月 31 日 24 点 0 分。

【描述】

time-range 命令用来创建一个时间段，来描述一个特定的时间范围。**undo time-range** 命令用来删除一个时间段。

缺省情况下，不存在任何时间段。

需要注意的是：

- 使用 **time-range** 命令时，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 256 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。
- 使用 *start-time* **to** *end-time days* 这组参数所创建的时间段为周期时间段，它将以一周为周期循环生效；使用 **from** *time1 date1* 和 **to** *time2 date2* 这组参数所创建的时间段为绝对时间段，它将在指定时间范围内生效；而同时使用了上述两组参数所创建的时间段，将取周期时间段和绝对时间段的交集作为生效的时间范围，譬如：创建一个时间段，既定义其在每周一的 8 点到 12 点生效，又定义其在 2010 年全年生效，那么其最终将在 2010 年全年内每周一的 8 点到 12 点生效。
- 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。

相关配置可参考命令 **display time-range**。

【举例】

创建名为 t1 的时间段，其时间范围为每周工作日的 8 点到 18 点。

```
<Sysname> system-view
[Sysname] time-range t1 8:0 to 18:0 working-day
```

创建名为 t2 的时间段，其时间范围为 2010 年全年。

```
<Sysname> system-view
[Sysname] time-range t2 from 0:0 1/1/2010 to 24:0 12/31/2010
```

创建名为 t3 的时间段，其时间范围为 2010 年全年内每周休息日的 8 点到 12 点。

```
<Sysname> system-view
[Sysname] time-range t3 8:0 to 12:0 off-day from 0:0 1/1/2010 to 24:0 12/31/2010
```

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

```
<Sysname> system-view
[Sysname] time-range t4 10:0 to 12:0 1 from 0:0 1/1/2010 to 24:0 1/31/2010
[Sysname] time-range t4 14:0 to 16:0 3 from 0:0 6/1/2010 to 24:0 6/30/2010
```