H3C IG 系列物联网网关

安全命令参考

新华三技术有限公司
http://www.h3c.com

资料版本：6W101-20191217
产品版本：R1227

Copyright © 2019 新华三技术有限公司及其许可者 版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。H3C 保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，H3C 尽全力在本手册中提供准确的信息，但是 H3C 并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

环境保护

本产品符合关于环境保护方面的设计要求，产品的存放、使用和弃置应遵照相关国家法律、法规要求进行。

前 言

本命令参考主要介绍 H3C IG 系列物联网网关产品的 ACL 命令、时间段命令以及 ARP 攻击防御命令。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

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

本书约定

1. 命令行格式约定

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

2. 图形界面格式约定

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

3. 各类标志

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

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

4. 图标约定

本书使用的图标及其含义如下：

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

5. 示例约定

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

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

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 ACL

1.1 ACL配置命令

1.1.1 acl

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

undo acl 命令用来删除指定或全部 ACL。

【命令】

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

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

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

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

【缺省情况】

不存在 ACL。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv6：指定 ACL 类型为 IPv6 ACL。

basic：指定创建基本 ACL。

advanced：指定创建高级 ACL。

mac：指定创建二层 ACL。

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

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

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

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

all：指定类型中全部 ACL。

【使用指导】

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

当 ACL 内不存在任何规则时，用户可以使用本命令对该 ACL 的规则匹配顺序进行修改，否则不允许进行修改。

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

【举例】

创建一个编号为 2000 的 IPv4 基本 ACL，并进入其视图。

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

创建一个 IPv4 基本 ACL，指定其名称为 flow，并进入其视图。

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

创建一个编号为 3000 的 IPv4 高级 ACL，并进入其视图。

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

创建一个编号为 2000 的 IPv6 基本 ACL，并进入其视图。

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

创建一个 IPv6 基本 ACL，其名称为 flow，并进入其视图。

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

创建一个 IPv6 高级 ACL，其名称为 abc，并进入其视图。

```
<Sysname> system-view
[Sysname] acl ipv6 advanced name abc
[Sysname-acl-ipv6-adv-abc]
```

创建一个编号为 4000 的二层 ACL，并进入其视图。

```
<Sysname> system-view
[Sysname] acl mac 4000
[Sysname-acl-mac-4000]
```

创建一个二层 ACL，其名称为 flow，并进入其视图。

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

【相关命令】

- **display acl**

1.1.2 acl copy

acl copy 命令用来复制并生成一个新的 ACL。

【命令】

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

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv6：指定 ACL 类型为 IPv6 ACL。

mac：指定 ACL 类型为二层 ACL。

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

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

name *source-acl-name*：指定源 ACL 的名称，该 ACL 必须存在。*source-acl-name* 为 1～63 个字符的字符串，不区分大小写。

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

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

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

【使用指导】

目的 ACL 的类型要与源 ACL 的类型相同。

除了 ACL 的编号或名称不同外，新生成的 ACL（即目的 ACL）的匹配顺序、规则匹配软件统计功能的开启情况、规则编号的步长、所包含的规则、规则的描述信息以及 ACL 的描述信息等都与源 ACL 的相同。

【举例】

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

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

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

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

```
[Sysname] acl copy name test to name paste
```

1.1.3 acl logging interval

acl logging interval 命令用来配置报文过滤日志信息的生成与发送周期，同时开启报文的首包上送功能。

undo acl logging interval 命令用来恢复缺省情况。

【命令】

acl logging interval *interval*

undo acl logging interval

【缺省情况】

报文过滤日志信息的生成与发送周期为 0 分钟，即不记录报文过滤的日志。报文首包上送功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval：报文过滤日志信息的生成与发送周期，取值范围为 0～1440，且必须为 5 的整数倍，0 表示不进行记录，单位为分钟。

【使用指导】

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

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

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

有关信息中心的详细介绍请参见“设备管理配置指导”中的“信息中心”。

【举例】

配置 IPv4 报文过滤日志的生成与发送周期为 10 分钟。

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

【相关命令】

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

1.1.4 acl trap interval

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

undo acl trap interval 命令用来恢复缺省情况。

【命令】

acl trap interval *interval*

undo acl trap interval

【缺省情况】

报文过滤告警信息的生成与发送周期为 0 分钟，即不记录报文过滤的告警信息。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval：报文过滤告警信息的生成与发送周期，取值范围为 0～1440，且必须为 5 的整数倍，0 表示不进行记录，单位为分钟。

【使用指导】

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

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

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

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

【举例】

配置 IPv4 报文过滤告警信息的生成与发送周期为 10 分钟。

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

【相关命令】

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

1.1.5 description

description 命令用来配置 ACL 的描述信息。

undo description 命令用来删除 ACL 的描述信息。

【命令】

description *text*

undo description

【缺省情况】

ACL 没有任何描述信息。

【视图】

IPv4 基本 ACL 视图/IPv4 高级 ACL 视图

IPv6 基本 ACL 视图/IPv6 高级 ACL 视图

二层 ACL 视图

【缺省用户角色】

network-admin

【参数】

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

【举例】

为 IPv4 基本 ACL 2000 配置描述信息。

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

【相关命令】

- **display acl**

1.1.6 display acl

display acl 命令用来显示 ACL 的配置和运行情况。

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

ipv6：指定 ACL 类型为 IPv6 ACL。

mac：指定 ACL 类型为二层 ACL。

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

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

all：显示指定类型中全部 ACL 的配置和运行情况。

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

【使用指导】

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

【举例】

显示所有 IPv4 ACL 的配置和运行情况。

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

表1-1 display acl 命令显示信息描述表

字段	描述
Basic IPv4 ACL 2001	该ACL的类型和编号，ACL的类型包括： • Basic IPv4 ACL：表示 IPv4 基本 ACL • Advanced IPv4 ACL：表示 IPv4 高级 ACL • Basic IPv6 ACL：表示 IPv6 基本 ACL • Advanced IPv6 ACL：表示 IPv6 高级 ACL • MAC ACL：表示二层 ACL
2 rules	该ACL内包含的规则数量
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 5 permit source 1.1.1.1 0	规则5的具体内容，源地址为具体地址
5 times matched	该规则匹配的次数为5（仅统计软件ACL的匹配次数，当匹配次数为0时不显示本字段）
rule 5 comment This rule is used on GigabitEthernet1/0/1.	规则5的描述信息
Dynamic	该规则由应用模块动态添加

1.1.7 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**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

interface [*interface-type interface-number*]：显示指定接口上 ACL 在报文过滤中的应用情况。*interface-type interface-number* 表示接口类型和接口编号。若未指定接口类型和接口编号，将显示除 VA（Virtual Access，虚拟访问）接口外所有接口上 ACL 在报文过滤中的应用情况。

当接口类型为以太网接口时，不需要指定 **slot** 参数。

inbound：显示入方向上 ACL 在报文过滤中的应用情况。

outbound：显示出方向上 ACL 在报文过滤中的应用情况。

【使用指导】

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

【举例】

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

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

表1-2 display packet-filter 命令显示信息描述表

字段	描述
Interface	ACL在指定接口上的应用情况
Inbound policy	ACL在入方向上的应用情况

字段	描述
Outbound policy	ACL在出方向上的应用情况
IPv4 ACL 2001	IPv4基本ACL 2001应用成功
IPv6 ACL 2002 (Failed)	IPv6基本ACL 2002应用失败
IPv4 default action	报文过滤的缺省动作，包括： • Deny：报文过滤缺省动作为 Deny 应用成功 • Deny (Failed)：报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit • Permit：报文过滤缺省动作为 Permit
IPv6 default action	报文过滤的缺省动作，包括： • Deny：报文过滤缺省动作为 Deny 应用成功 • Deny (Failed)：报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit • Permit：报文过滤缺省动作为 Permit
MAC default action	报文过滤的缺省动作，包括： • Deny：报文过滤缺省动作为 Deny 应用成功 • Deny (Failed)：报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit • Permit：报文过滤缺省动作为 Permit

1.1.8 display packet-filter statistics

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

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

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

inbound：显示入方向上的统计信息。

outbound：显示出方向上的统计信息。

default：显示报文过滤缺省动作的统计信息。

ipv6：指定 ACL 类型为 IPv6 ACL。

mac：指定 ACL 类型为二层 ACL。

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

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

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

brief：显示简要统计信息。

【使用指导】

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

【举例】

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

```
<Sysname> display packet-filter statistics interface gigabitethernet 1/0/1 inbound
Interface: GigabitEthernet1/0/1
 Inbound policy:
  IPv4 ACL 2001
   From 2011-06-04 10:25:21 to 2011-06-04 10:35:57
   rule 0 permit source 2.2.2.2 0 counting (2 packets, 256 bytes)
   rule 5 permit source 1.1.1.1 0 counting (Failed)
   Totally 2 packets 256 bytes permitted, 0 packets 0 bytes denied
   Totally 100% permitted, 0% denied

  IPv6 ACL 2000

  MAC ACL 4000
   rule 0 permit

  IPv4 default action: Deny
   From 2011-06-04 10:25:21 to 2011-06-04 10:35:57
   Totally 7 packets

  IPv6 default action: Deny
   From 2011-06-04 10:25:41 to 2011-06-04 10:35:57
   Totally 0 packets
  MAC default action: Deny
   From 2011-06-04 10:25:34 to 2011-06-04 10:35:57
   Totally 0 packets
```

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

字段	描述
Interface	在指定接口上应用的统计信息
Inbound policy	在入方向上应用的统计信息

字段	描述
Outbound policy	在出方向上应用的统计信息
IPv4 ACL 2001	IPv4基本ACL 2001应用成功
IPv4 ACL 2002 (Failed)	IPv4基本ACL 2002应用失败
2 packets	该规则匹配了2个包（当匹配的包个数为0时不显示本字段）
rule 5 permit source 1.1.1.10 (Failed)	规则5应用失败
Totally 2 packets permitted, 0 packets denied	该ACL允许和拒绝符合条件报文的个数
Totally 100% permitted, 0% denied	该ACL允许符合条件报文的通过率和拒绝符合条件报文的丢弃率
IPv4 default action	报文过滤的缺省动作，包括： • Deny：报文过滤缺省动作为 Deny 应用成功 • Deny (Failed)：报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit • Permit：报文过滤缺省动作为 Permit
IPv6 default action	报文过滤的缺省动作，包括： • Deny：报文过滤缺省动作为 Deny 应用成功 • Deny (Failed)：报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit • Permit：报文过滤缺省动作为 Permit
MAC default action	报文过滤的缺省动作，包括： • Deny：报文过滤缺省动作为 Deny 应用成功 • Deny (Failed)：报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit • Permit：报文过滤缺省动作为 Permit

【相关命令】

- **reset packet-filter statistics**

1.1.9 display packet-filter statistics sum

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

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

inbound：显示入方向上 ACL 在报文过滤中应用的累加统计信息。

outbound：显示出方向上 ACL 在报文过滤中应用的累加统计信息。

ipv6：指定 ACL 类型为 IPv6 ACL。

mac：指定 ACL 类型为二层 ACL。

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

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

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

brief：显示 ACL 在报文过滤中应用的简要累加统计信息。

【举例】

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

```
<Sysname> display packet-filter statistics sum inbound 2001
Sum:
 Inbound policy:
  IPv4 ACL 2001
   rule 0 permit source 2.2.2.2 0 counting (2 packets, 256 bytes)
   rule 5 permit source 1.1.1.1 0
   Totally 2 packets 256 bytes permitted, 0 packets 0 bytes denied
   Totally 100% permitted, 0% denied
```

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

```
<Sysname> display packet-filter statistics sum inbound 2000 brief
Sum:
 Inbound policy:
  IPv4 ACL 2000
   Totally 2 packets 256 bytes permitted, 0 packets 0 bytes denied
   Totally 100% permitted, 0% denied
```

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

字段	描述
Sum	ACL在报文过滤中应用的累加统计信息
Inbound policy	ACL在入方向上应用的累加统计信息
Outbound policy	ACL在出方向上应用的累加统计信息
IPv4 ACL 2001	IPv4基本ACL 2001应用的累加统计信息
2 packets, 256 bytes	该规则匹配了2个包，共256字节（当匹配的包个数为0时不显示本字段）
Totally 2 packets 256 bytes permitted, 0 packets 0 bytes denied	该ACL允许和拒绝符合条件报文的个数及字节数
Totally 100% permitted, 0% denied	该ACL允许符合条件报文的通过率和拒绝符合条件报文的丢弃率

【相关命令】

- **reset packet-filter statistics**

1.1.10 display packet-filter verbose

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

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

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

inbound：显示入方向上 ACL 在报文过滤中的详细应用情况。

outbound：显示出方向上 ACL 在报文过滤中的详细应用情况。

ipv6：指定 ACL 类型为 IPv6 ACL。

mac：指定 ACL 类型为二层 ACL。

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

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

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

【使用指导】

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

【举例】

显示接口 GigabitEthernet1/0/1 入方向上全部 ACL 在报文过滤中的详细应用情况。

```
<Sysname> display packet-filter verbose interface gigabitethernet 1/0/1 inbound
Interface: GigabitEthernet1/0/1
 Inbound policy:
  IPv4 ACL 2001
```

```
 rule 0 permit
 rule 5 permit source 1.1.1.1 0 (Failed)

IPv6 ACL 2000
 rule 0 permit

MAC ACL 4000

IPv4 default action: Deny

IPv6 default action: Deny

MAC default action: Deny
```

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

字段	描述
Interface	ACL在指定接口上的详细应用情况
Inbound policy	ACL在入方向上的详细应用情况
Outbound policy	ACL在出方向上的详细应用情况
IPv4 ACL 2001	IPv4基本ACL 2001应用成功
IPv4 ACL 2002 (Failed)	IPv4基本ACL 2002应用失败
rule 5 permit source 1.1.1.1 0 (Failed)	规则5应用失败
IPv4 default action	报文过滤的缺省动作，包括： • Deny：报文过滤缺省动作为 Deny 应用成功 • Deny (Failed)：报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit • Permit：报文过滤缺省动作为 Permit
IPv6 default action	报文过滤的缺省动作，包括： • Deny：报文过滤缺省动作为 Deny 应用成功 • Deny (Failed)：报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit • Permit：报文过滤缺省动作为 Permit
MAC default action	报文过滤的缺省动作，包括： • Deny：报文过滤缺省动作为 Deny 应用成功 • Deny (Failed)：报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit • Permit：报文过滤缺省动作为 Permit

1.1.11 packet-filter

packet-filter 命令用来在接口上应用 ACL 进行报文过滤。

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

【命令】

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

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

【缺省情况】

接口不对报文进行过滤。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6：指定 ACL 类型为 IPv6 ACL。

mac：指定 ACL 类型为二层 ACL。

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

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

name *acl-name*：指定 ACL 的名称。*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写。

inbound：对收到的报文进行过滤。

outbound：对发出的报文进行过滤。

【使用指导】

【举例】

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

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

【相关命令】

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

1.1.12 packet-filter default deny

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

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

【命令】

packet-filter default deny

undo packet-filter default deny

【缺省情况】

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

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

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

【举例】

配置报文过滤的缺省动作为 Deny。

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

【相关命令】

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

1.1.13 reset acl counter

reset acl counter 命令用来清除 ACL 的统计信息。

【命令】

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

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

ipv6：指定 ACL 类型为 IPv6 ACL。

mac：指定 ACL 类型为二层 ACL。

acl-number：清除指定编号 ACL 的统计信息。*acl-number* 表示 ACL 的编号，取值范围及其代表的 ACL 类型如下：

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

- 4000～4999：表示二层 ACL。

all：清除指定类型中全部 ACL 的统计信息。

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

【举例】

清除 IPv4 基本 ACL 2001 的统计信息。

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

【相关命令】

- **display acl**

1.1.14 reset packet-filter statistics

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

【命令】

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

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

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

inbound：清除入方向上的统计信息。

outbound：清除出方向上的统计信息。

default：清除缺省动作在报文过滤中应用的统计信息。

ipv6：指定 ACL 类型为 IPv6 ACL。

mac：指定 ACL 类型为二层 ACL。

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

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

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

【使用指导】

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

【举例】

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

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

【相关命令】

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

1.1.15 rule (IPv4 advanced ACL view)

rule 命令用来为 IPv4 高级 ACL 创建一条规则。

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

【命令】

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

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

undo rule [*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** | **time-range** *time-range-name*] *

【缺省情况】

IPv4 高级 ACL 内不存在任何规则。

【视图】

IPv4 高级 ACL 视图

【缺省用户角色】

network-admin

【参数】

rule-id：指定 IPv4 高级 ACL 规则的编号，取值范围为 0～65534。若未指定本参数，系统将从规则编号的起始值开始，自动分配一个大于现有最大编号的步长最小倍数。譬如现有规则的最大编号为 28，步长为 5，那么自动分配的新编号将是 30。

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

protocol：表示 IPv4 承载的协议类型，可输入的形式如下：

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

*protocol*之后可配置如 表 1-6 所示的规则信息参数。

表1-6 规则信息参数

参数	类别	作用	说明
source { *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 *source-wildcard*：源IP地址的通配符掩码（为0表示主机地址） **any**：任意源IP地址
destination { *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 *dest-wildcard*：目的IP地址的通配符掩码（为0表示主机地址） **any**：任意目的IP地址
counting	统计	开启规则匹配软件统计功能，缺省为关闭	
precedence *precedence*	报文优先级	指定IP优先级	*precedence*用数字表示时，取值范围为0～7；用字符表示时，分别对应**routine**、**priority**、**immediate**、**flash**、**flash-override**、**critical**、**internet**、**network**
tos *tos*	报文优先级	指定ToS优先级	*tos*用数字表示时，取值范围为0～15；用字符表示时，可以选取**max-reliability**（2）、**max-throughput**（4）、**min-delay**（8）、**min-monetary-cost**（1）、**normal**（0）
dscp *dscp*	报文优先级	指定DSCP优先级	*dscp*用数字表示时，取值范围为0～63；用字符表示时，可以选取**af11**（10）、**af12**（12）、**af13**（14）、**af21**（18）、**af22**（20）、**af23**（22）、**af31**（26）、**af32**（28）、**af33**（30）、**af41**（34）、**af42**（36）、**af43**（38）、**cs1**（8）、**cs2**（16）、**cs3**（24）、**cs4**（32）、**cs5**（40）、**cs6**（48）、**cs7**（56）、**default**（0）、**ef**（46）。

参数	类别	作用	说明
fragment	分片信息	仅对分片报文的非首个分片有效，而对非分片报文和分片报文的首个分片无效	若未指定该参数，则表示该规则对所有报文（包括非分片报文和分片报文的每个分片）均有效
logging	日志操作	表示记录规则匹配报文的日志信息，包括匹配报文的规则和匹配报文的个数	该功能需要使用该ACL的模块支持日志记录功能，例如报文过滤
time-range *time-range-name*	时间段	指定本规则生效的时间段	*time-range-name*：时间段的名称，为1～32个字符的字符串，不区分大小写。若该时间段尚未配置，该规则仍会成功创建但系统将给出提示信息，并在该时间段的配置完成后此规则才会生效。有关时间段的详细介绍和具体配置过程，请参见“安全配置指导”中的“时间段”

当*protocol*为**tcp**（6）或**udp**（17）时，用户还可配置如 表 1-7 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*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 *port1*、*port2*：TCP或UDP的端口号，用数字表示时，取值范围为0～65535；用字符表示时，TCP端口号可以选取**chargen**（19）、**bgp**（179）、**cmd**（514）、**daytime**（13）、**discard**（9）、**dns**（53）、**domain**（53）、**echo**（7）、**exec**（512）、**finger**（79）、**ftp**（21）、**ftp-data**（20）、**gopher**（70）、**hostname**（101）、**irc**（194）、**klogin**（543）、**kshell**（544）、**login**（513）、**lpd**（515）、**nntp**（119）、**pop2**（109）、**pop3**（110）、**smtp**（25）、**sunrpc**（111）、**tacacs**（49）、**talk**（517）、**telnet**（23）、**time**（37）、**uucp**（540）、**whois**（43）、**www**（80）；UDP端口号可以选取**biff**（512）、**bootpc**（68）、**bootps**（67）、**discard**（9）、**dns**（53）、**dnsix**（90）、**echo**（7）、**mobilip-ag**（434）、**mobilip-mn**（435）、**nameserver**（42）、**netbios-dgm**（138）、**netbios-ns**（137）、**netbios-ssn**（139）、**ntp**（123）、**rip**（520）、**snmp**（161）、**snmptrap**（162）、**sunrpc**（111）、**syslog**（514）、**tacacs-ds**（65）、**talk**（517）、**tftp**（69）、**time**（37）、**who**（513）、**xdmcp**（177）
destination-port *operator port1* [*port2*]	目的端口	定义TCP/UDP报文的目的端口信息	

参数	类别	作用	说明
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	TCP报文标识	定义对携带不同标志位（包括ACK、FIN、PSH、RST、SYN和URG六种）的TCP报文的处理规则	TCP协议特有的参数。表示匹配携带不同标志位的TCP报文，各*value*的取值可为0或1（0表示不携带此标志位，1表示携带此标志位） 对于一条规则中各标志位的配置组合，按照“或”的规则进行匹配。譬如：当配置为**ack** 0 **psh** 1时，匹配不携带ACK或携带PSH标志位的TCP报文
established	TCP连接建立标识	定义对TCP连接报文的处理规则	TCP协议特有的参数。表示匹配携带ACK或RST标志位的TCP连接报文

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

表1-8 ICMP 特有的规则信息参数

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

表1-9 ICMP 消息名称与消息类型和消息码的对应关系

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

ICMP 消息名称	ICMP 消息类型	ICMP 消息码
source-route-failed	3	5
timestamp-reply	14	0
timestamp-request	13	0
ttl-exceeded	11	0

【使用指导】

使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。

创建的规则若与动态规则的内容完全相同，则会覆盖已有动态规则。

新创建或修改的规则不能与已有规则的内容完全相同，否则将提示出错，并导致该操作失败。

当 ACL 的规则匹配顺序为配置顺序时，允许修改该 ACL 内的任意一条已有规则；当 ACL 的规则匹配顺序为自动排序时，不允许修改该 ACL 内的已有规则，否则将提示出错。

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

删除规则时需要注意的是：

- 使用 **undo rule** *rule-id* 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- **undo rule** [*rule-id*] { **deny** | **permit** }命令无法删除规则中的部分内容，使用 **undo rule** { **deny** | **permit** }命令时，必须输入已存在规则的完整形式。

【举例】

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

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

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

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

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

```
<Sysname> system-view
[Sysname] acl advanced 3002
[Sysname-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp
[Sysname-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp-data
[Sysname-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp
[Sysname-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp-data
```

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

```
<Sysname> system-view
[Sysname] acl advanced 3003
[Sysname-acl-ipv4-adv-3003] rule permit udp source-port eq snmp
[Sysname-acl-ipv4-adv-3003] rule permit udp source-port eq snmptrap
[Sysname-acl-ipv4-adv-3003] rule permit udp destination-port eq snmp
[Sysname-acl-ipv4-adv-3003] rule permit udp destination-port eq snmptrap
```

【相关命令】

- **acl**
- **acl logging interval**
- **display acl**
- **step**
- **time-range**（安全命令参考/时间段）

1.1.16 rule (IPv4 basic ACL view)

rule 命令用来为 IPv4 基本 ACL 创建一条规则。

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

【命令】

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

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

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

【缺省情况】

IPv4 基本 ACL 内不存在任何规则。

【视图】

IPv4 基本 ACL 视图

【缺省用户角色】

network-admin

【参数】

rule-id：指定 IPv4 基本 ACL 规则的编号，取值范围为 0～65534。若未指定本参数，系统将从规则编号的起始值开始，自动分配一个大于现有最大编号的步长最小倍数。譬如现有规则的最大编号为 28，步长为 5，那么自动分配的新编号将是 30。

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

counting：表示开启规则匹配软件统计功能，缺省为关闭。

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

logging：表示记录规则匹配报文的日志信息，包括匹配报文的规则和匹配报文的个数。该功能需要使用该 ACL 的模块支持日志记录功能，例如报文过滤。

source { *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。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“安全配置指导”中的“时间段”。

【使用指导】

使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。

新创建或修改的规则不能与已有规则的内容完全相同，否则将提示出错，并导致该操作失败。

当 ACL 的规则匹配顺序为配置顺序时，允许修改该 ACL 内的任意一条已有规则；当 ACL 的规则匹配顺序为自动排序时，不允许修改该 ACL 内的已有规则，否则将提示出错。

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

删除规则时需要注意的是：

- 使用 **undo rule** *rule-id* 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- **undo rule** [*rule-id*] { **deny** | **permit** }命令无法删除规则中的部分内容，使用 **undo rule** { **deny** | **permit** }命令时，必须输入已存在规则的完整形式。

【举例】

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

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

【相关命令】

- **acl**
- **acl logging interval**
- **display acl**
- **step**
- **time-range**（安全命令参考/时间段）

1.1.17 rule (IPv6 advanced ACL view)

rule 命令用来为 IPv6 高级 ACL 创建一条规则。

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

【命令】

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

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

undo rule [*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*] *

【缺省情况】

IPv6 高级 ACL 内不存在任何规则。

【视图】

IPv6 高级 ACL 视图

【缺省用户角色】

network-admin

【参数】

rule-id：指定 IPv6 高级 ACL 规则的编号，取值范围为 0～65534。若未指定本参数，系统将从规则编号的起始值开始，自动分配一个大于现有最大编号的步长最小倍数。譬如现有规则的最大编号为 28，步长为 5，那么自动分配的新编号将是 30。

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

protocol：表示 IPv6 承载的协议类型，可输入的形式如下：

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

*protocol*之后可配置如 表 1-10 所示的规则信息参数。

表1-10 规则信息参数

参数	类别	作用	说明
source { *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	开启规则匹配软件统计功能，缺省为关闭	
dscp *dscp*	报文优先级	指定DSCP优先级	*dscp*：用数字表示时，取值范围为0～63；用名称表示时，可选取**af11**（10）、**af12**（12）、**af13**（14）、**af21**（18）、**af22**（20）、**af23**（22）、**af31**（26）、**af32**（28）、**af33**（30）、**af41**（34）、**af42**（36）、**af43**（38）、**cs1**（8）、**cs2**（16）、**cs3**（24）、**cs4**（32）、**cs5**（40）、**cs6**（48）、**cs7**（56）、**default**（0）或**ef**（46）
flow-label *flow-label-value*	流标签字段	指定IPv6基本报文头中流标签字段的值	*flow-label-value*：流标签字段的值，取值范围为0～1048575
fragment	报文分片	仅对分片报文的非首个分片有效，而对非分片报文和分片报文的首个分片无效	若未指定本参数，表示该规则对所有报文（包括非分片报文和分片报文的每个分片）均有效
logging	日志操作	表示记录规则匹配报文的日志信息，包括匹配报文的规则和匹配报文的个数	该功能需要使用该ACL的模块支持日志记录功能，例如报文过滤
routing [**type** *routing-type*]	路由头	指定路由头的类型	*routing-type*：路由头类型的值，取值范围为0～255 若指定了**type** *routing-type*参数，表示仅对指定类型的路由头有效；否则，表示对IPv6所有类型的路由头都有效

参数	类别	作用	说明
hop-by-hop [**type** *hop-type*]	逐跳头	指定逐跳头的类型	*hop-type*：逐跳头类型的值，取值范围为0～255 若指定了**type** *hop-type*参数，表示仅对指定类型的逐跳头有效；否则，表示对IPv6所有类型的逐跳头都有效
time-range *time-range-name*	时间段	指定本规则生效的时间段	*time-range-name*：时间段的名称，为1～32个字符的字符串，不区分大小写。若该时间段尚未配置，该规则仍会成功创建但系统将给出提示信息，并在该时间段的配置完成后此规则才会生效。有关时间段的详细介绍和具体配置过程，请参见“安全配置指导”中的“时间段”

当*protocol*为**tcp**（6）或**udp**（17）时，用户还可配置如 表 1-11 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）、**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） 对于一条规则中各标志位的配置组合，按照“或”的规则进行匹配。譬如：当配置为**ack** 0 **psh** 1时，匹配不携带ACK或携带PSH标志位的TCP报文

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

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

表1-12 ICMPv6 特有的规则信息参数

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

表1-13 ICMPv6 消息名称与消息类型和消息码的对应关系

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

【使用指导】

使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。

创建的规则若与动态规则的内容完全相同，则会覆盖已有动态规则。新创建或修改的规则不能与已有规则的内容完全相同，否则将提示出错，并导致该操作失败。

当 ACL 的规则匹配顺序为配置顺序时，允许修改该 ACL 内的任意一条已有规则；当 ACL 的规则匹配顺序为自动排序时，不允许修改该 ACL 内的已有规则，否则将提示出错。

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

删除规则时需要注意的是：

- 使用 **undo rule** *rule-id* 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- **undo rule** [*rule-id*] { **deny** | **permit** }命令无法删除规则中的部分内容，使用 **undo rule { deny | permit }**命令时，必须输入已存在规则的完整形式。

【举例】

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

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

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

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

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

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

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

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

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

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

【相关命令】

- **acl**
- **acl logging interval**
- **display acl**
- **step**
- **time-range**（安全命令参考/时间段）

1.1.18 rule (IPv6 basic ACL view)

rule 命令用来为 IPv6 基本 ACL 创建一条规则。

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

【命令】

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

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

undo rule [*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*] *

【缺省情况】

IPv6 基本 ACL 内不存在任何规则。

【视图】

IPv6 基本 ACL 视图

【缺省用户角色】

network-admin

【参数】

rule-id：指定 IPv6 基本 ACL 规则的编号，取值范围为 0～65534。若未指定本参数，系统将从规则编号的起始值开始，自动分配一个大于现有最大编号的步长最小倍数。譬如现有规则的最大编号为 28，步长为 5，那么自动分配的新编号将是 30。

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

counting：表示开启规则匹配软件统计功能，缺省为关闭。

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

logging：表示记录规则匹配报文的日志信息，包括匹配报文的规则和匹配报文的个数。该功能需要使用该 ACL 的模块支持日志记录功能，例如报文过滤。

routing [**type** *routing-type*]：表示对所有或指定类型的路由头有效，*routing-type* 表示路由头类型的值，取值范围为 0～255。若指定了 **type** *routing-type* 参数，表示仅对指定类型的路由头有效；否则，表示对 IPv6 所有类型的路由头都有效。

source { *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。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“安全配置指导”中的“时间段”。

【使用指导】

使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。

新创建或修改的规则不能与已有规则的内容完全相同，否则将提示出错，并导致该操作失败。

当 ACL 的规则匹配顺序为配置顺序时，允许修改该 ACL 内的任意一条已有规则；当 ACL 的规则匹配顺序为自动排序时，不允许修改该 ACL 内的已有规则，否则将提示出错。

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

删除规则时需要注意的是：

- 使用 **undo rule** *rule-id* 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- **undo rule** [*rule-id*] { **deny** | **permit** }命令无法删除规则中的部分内容，使用 **undo rule** { **deny** | **permit** }命令时，必须输入已存在规则的完整形式。

【举例】

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

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

【相关命令】

- **acl**
- **acl logging interval**
- **display acl**
- **step**
- **time-range**（安全命令参考/时间段）

1.1.19 rule (Layer 2 ACL view)

rule 命令用来为二层 ACL 创建一条规则。

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

【命令】

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

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

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

【缺省情况】

二层 ACL 内不存在任何规则。

【视图】

二层 ACL 视图

【缺省用户角色】

network-admin

【参数】

rule-id：指定二层 ACL 规则的编号，取值范围为 0～65534。若未指定本参数，系统将从规则编号的起始值开始，自动分配一个大于现有最大编号的步长最小倍数。譬如现有规则的最大编号为 28，步长为 5，那么自动分配的新编号将是 30。

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

cos *dot1p*：指定 802.1p 优先级。*dot1p* 表示 802.1p 优先级，可输入的形式如下：

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

counting：表示开启规则匹配软件统计功能，缺省为关闭。

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

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

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

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

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

【使用指导】

使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。

新创建或修改的规则不能与已有规则的内容完全相同，否则将提示出错，并导致该操作失败。

当 ACL 的规则匹配顺序为配置顺序时，允许修改该 ACL 内的任意一条已有规则；当 ACL 的规则匹配顺序为自动排序时，不允许修改该 ACL 内的已有规则，否则将提示出错。

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

删除规则时需要注意的是：

- 使用 **undo rule** *rule-id* 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- **undo rule** [*rule-id*] { **deny** | **permit** }命令无法删除规则中的部分内容，使用 **undo rule** { **deny** | **permit** }命令时，必须输入已存在规则的完整形式。

【举例】

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

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

【相关命令】

- **acl**
- **display acl**
- **step**
- **time-range**（安全命令参考/时间段）

1.1.20 rule comment

rule comment 命令用来为规则配置描述信息。

undo rule comment 命令用来删除指定规则的描述信息。

【命令】

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

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

【缺省情况】

规则没有描述信息。

【视图】

IPv4 基本 ACL 视图/IPv4 高级 ACL 视图

IPv6 基本 ACL 视图/IPv6 高级 ACL 视图

二层 ACL 视图

【缺省用户角色】

network-admin

【参数】

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

text：表示规则的描述信息，为 1～127 个字符的字符串，区分大小写。

【使用指导】

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

【举例】

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

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule 0 deny source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2000] rule 0 comment This rule is used on gigabitethernet 1/0/1.
```

【相关命令】

- **display acl**

1.1.21 step

step 命令用来配置规则编号的步长。

undo step 命令用来恢复缺省情况。

【命令】

step *step-value*

undo step

【缺省情况】

规则编号的步长为 5，起始值为 0。

【视图】

IPv4 基本 ACL 视图/IPv4 高级 ACL 视图

IPv6 基本 ACL 视图/IPv6 高级 ACL 视图

二层 ACL 视图

【缺省用户角色】

network-admin

【参数】

step-value：表示规则编号的步长值，取值范围为 1～20。

【使用指导】

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

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

【举例】

将 IPv4 基本 ACL 2000 的规则编号的步长配置为 2。

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

【相关命令】

- **display acl**

目 录

1 时间段

1.1 时间段配置命令

1.1.1 display time-range

display time-range 命令用来显示时间段的配置和状态信息。

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

time-range-name：显示指定名称时间段的配置和状态信息。*time-range-name* 表示时间段的名称，为 1～32 个字符的字符串，使用英文字母时不区分大小写。

all：显示所有时间段的配置和状态信息。

【举例】

显示时间段 t4 的配置和状态信息。

```
<Sysname> display time-range t4
Current time is 17:12:34 11/23/2010 Tuesday

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

表1-1 display time-range 命令显示信息描述表

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

1.1.2 time-range

time-range 命令用来创建一个时间段，来描述一个特定的时间范围。如果指定的时间段已经创建，则本命令可以修改时间段的时间范围。

undo time-range 命令用来删除一个时间段。

【命令】

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

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

【缺省情况】

不存在时间段。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

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

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

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

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

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

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

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

【使用指导】

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

在一个时间段中，可以使用以下两种方式定义时间范围：

- 使用 *start-time* **to** *end-time days* 这组参数所创建的时间段为周期时间段，它将以一周为周期循环生效。
- 使用 **from** *time1 date1* 和 **to** *time2 date2* 这组参数所创建的时间段为绝对时间段，它将在指定时间范围内生效。

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

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

【举例】

创建名为 t1 的时间段，其时间范围为每周工作日的 8 点到 18 点。

```
<Sysname> system-view
[Sysname] time-range t1 08:00 to 18:00 working-day
```

创建名为 t2 的时间段，其时间范围为 2011 年全年。

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

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

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

创建名为 t4 的时间段，其时间范围为 2011 年 1 月和 6 月内每周一的 10 点到 12 点以及每周三的 14 到 16 点。

```
<Sysname> system-view
[Sysname] time-range t4 10:00 to 12:00 1 from 00:00 1/1/2011 to 24:00 1/31/2011
[Sysname] time-range t4 14:00 to 16:00 3 from 00:00 6/1/2011 to 24:00 6/30/2011
```

【相关命令】

- **display time-range**

目 录

1 ARP攻击防御

1.1 ARP防止IP报文攻击配置命令

1.1.1 arp resolving-route enable

arp resolving-route enable 命令用来开启 ARP 黑洞路由功能。

undo arp resolving-route enable 命令用来关闭 ARP 黑洞路由功能。

【命令】

arp resolving-route enable

undo arp resolving-route enable

【缺省情况】

ARP 黑洞路由功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

建议在网关设备上开启本功能。

【举例】

开启 ARP 黑洞路由功能。

```
<Sysname> system-view
[Sysname] arp resolving-route enable
```

【相关命令】

- **arp resolving-route probe-count**
- **arp resolving-route probe-interval**

1.1.2 arp resolving-route probe-count

arp resolving-route probe-count 命令用来配置发送 ARP 请求报文的次数。

undo arp resolving-route probe-count 命令用来恢复缺省情况。

【命令】

arp resolving-route probe-count *count*

undo arp resolving-route probe-count

【缺省情况】

发送 ARP 请求报文的次数为 3 次。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

count：发送 ARP 请求报文的次数，取值范围为 1～25。

【举例】

配置发送 ARP 请求报文的次数为 5 次。

```
<Sysname> system-view
[Sysname] arp resolving-route probe-count 5
```

【相关命令】

- **arp resolving-route enable**
- **arp resolving-route probe-interval**

1.1.3 arp resolving-route probe-interval

arp resolving-route probe-interval 命令用来配置发送 ARP 请求报文的时间间隔。

undo arp resolving-route probe-interval 命令用来恢复缺省情况。

【命令】

arp resolving-route probe-interval *interval*

undo arp resolving-route probe-interval

【缺省情况】

发送 ARP 请求报文的时间间隔是 1 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval：发送 ARP 请求报文的时间间隔，取值范围为 1～5，单位为秒。

【举例】

配置发送 ARP 请求报文的时间间隔为 3 秒。

```
<Sysname> system-view
[Sysname] arp resolving-route probe-interval 3
```

【相关命令】

- **arp resolving-route enable**
- **arp resolving-route probe-count**

1.1.4 arp source-suppression enable

arp source-suppression enable 命令用来开启 ARP 源地址抑制功能。

undo arp source-suppression enable 命令用来关闭 ARP 源地址抑制功能。

【命令】

arp source-suppression enable

undo arp source-suppression enable

【缺省情况】

ARP 源地址抑制功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

建议在网关设备上开启本功能。

【举例】

开启 ARP 源地址抑制功能。

```
<Sysname> system-view
[Sysname] arp source-suppression enable
```

【相关命令】

- **display arp source-suppression**

1.1.5 arp source-suppression limit

arp source-suppression limit 命令用来配置 ARP 源抑制的阈值。

undo arp source-suppression limit 命令用来恢复缺省情况。

【命令】

arp source-suppression limit *limit-value*

undo arp source-suppression limit

【缺省情况】

ARP 源抑制的阈值为 10。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

limit-value：ARP 源抑制的阈值，即设备在 5 秒间隔内可以处理的源 IP 相同，但目的 IP 地址不能解析的 IP 报文的最大数目，取值范围为 2～1024。

【使用指导】

如果网络中每 5 秒内从某 IP 地址向设备某接口发送目的 IP 地址不能解析的 IP 报文超过了设置的阈值，则设备将不再处理由此 IP 地址发出的 IP 报文直至该 5 秒结束，从而避免了恶意攻击所造成的危害。

【举例】

配置 ARP 源抑制的阈值为 100。

```
<Sysname> system-view
[Sysname] arp source-suppression limit 100
```

【相关命令】

- **display arp source-suppression**

1.1.6 display arp source-suppression

display arp source-suppression 命令用来显示当前 ARP 源抑制的配置信息。

【命令】

display arp source-suppression

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【举例】

显示当前 ARP 源抑制的配置信息。

```
<Sysname> display arp source-suppression
 ARP source suppression is enabled
 Current suppression limit: 100
```

表1-1 display arp source-suppression 显示信息描述表

字段	描述
ARP source suppression is enabled	ARP源抑制功能处于开启状态
Current suppression limit	设备在5秒时间间隔内可以接收到的源IP相同，但目的IP地址不能解析的IP报文的最大数目

1.2 ARP报文限速配置命令

1.2.1 arp rate-limit

arp rate-limit 命令用来开启 ARP 报文限速功能，并设置 ARP 报文限速速率。

undo arp rate-limit 命令用来关闭 ARP 报文限速功能。

【命令】

arp rate-limit [*pps*]

undo arp rate-limit

【缺省情况】

ARP 报文限速功能处于开启状态。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

pps：ARP 限速速率，单位为包每秒（pps），取值范围为 5～3072。如果未指定本参数，则不进行 ARP 限速。

【使用指导】

不指定限速速率时，设备使用缺省限速速率，超过限速部分的报文会被丢弃。

【举例】

在二层以太网接口 GigabitEthernet1/0/1 上开启 ARP 报文限速功能，并设置 ARP 报文限速速率为 50pps。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp rate-limit 50
```

1.2.2 arp rate-limit log enable

arp rate-limit log enable 命令用来开启 ARP 报文限速日志功能。

undo arp rate-limit log enable 命令用来关闭 ARP 报文限速日志功能。

【命令】

arp rate-limit log enable

undo arp rate-limit log enable

【缺省情况】

设备的 ARP 报文限速日志功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

当开启了 ARP 限速日志功能后，设备将这个时间间隔内的超速峰值作为日志的速率值发送到设备的信息中心，通过设置信息中心的参数，最终决定日志报文的输出规则（即是否允许输出以及输出方向）。有关信息中心参数的设置请参见“设备管理配置指导”中的“信息中心”。

【举例】

开启 ARP 报文限速日志功能。

```
<Sysname> system-view
[Sysname] arp rate-limit log enable
```

1.2.3 arp rate-limit log interval

arp rate-limit log interval 命令用来配置当设备收到的 ARP 报文速率超过用户设定的限速值时，设备发送告警和日志的时间间隔。

undo arp rate-limit log interval 命令用来恢复缺省情况。

【命令】

arp rate-limit log interval *interval*

undo arp rate-limit log interval

【缺省情况】

当设备收到的 ARP 报文速率超过用户设定的限速值时，设备发送告警和日志的时间间隔为 60 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval：当端口上的 ARP 报文速率超过用户设定的限速值时，设备发送告警和日志的时间间隔。取值范围为 1～86400，单位为秒。

【使用指导】

用户需要先开启发送告警或日志功能，然后配置此命令指定设备发送告警和日志的时间间隔，同时本命令必须和端口下的 **arp rate-limit** 命令配合使用，单独配置本命令无效。

【举例】

当设备收到的 ARP 报文速率超过用户设定的限速值时，配置设备发送告警和日志的时间间隔为 120 秒。

```
<Sysname> system-view
[Sysname] arp rate-limit log interval 120
```

【相关命令】

- **arp rate-limit**

- **arp rate-limit log enable**
- **snmp-agent trap enable arp**

1.2.4 snmp-agent trap enable arp

snmp-agent trap enable arp 命令用来开启 ARP 模块的告警功能。

undo snmp-agent trap enable arp 命令用来关闭 ARP 模块的告警功能。

【命令】

snmp-agent trap enable arp [rate-limit]

undo snmp-agent trap enable arp [rate-limit]

【缺省情况】

ARP 模块的告警功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

rate-limit：开启 ARP 报文限速的告警功能。

【使用指导】

当开启了 ARP 模块的告警功能后，设备将这个时间间隔内的超速峰值作为告警信息发送出去，生成的告警信息将发送到设备的 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关特性。

有关告警信息的详细描述，请参见“网络管理和监控配置指导”中的“SNMP”。

【举例】

开启 ARP 报文限速的告警功能。

```
<Sysname> system-view
[Sysname] snmp-agent trap enable arp rate-limit
```

1.3 源MAC地址固定的ARP攻击检测配置命令

1.3.1 arp source-mac

arp source-mac 命令用来开启源 MAC 地址固定的 ARP 攻击检测功能，并选择检查模式。

undo arp source-mac 命令用来关闭源 MAC 地址固定的 ARP 攻击检测功能。

【命令】

arp source-mac { filter | monitor }

undo arp source-mac [filter | monitor]

【缺省情况】

源 MAC 地址固定的 ARP 攻击检测功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

filter：配置检查方式为过滤模式。

monitor：配置检查方式为监控模式。

【使用指导】

建议在网关设备上开启本功能。

本特性根据 ARP 报文的源 MAC 地址对上送 CPU 的 ARP 报文进行统计，在 5 秒内，如果收到同一源 MAC 地址（源 MAC 地址固定）的 ARP 报文超过一定的阈值，则认为存在攻击，系统会将此 MAC 地址添加到攻击检测表项中。当开启了 ARP 日志信息功能（配置 **arp check log enable** 命令），且在该攻击检测表项老化之前，如果设置的检查模式为过滤模式，则会打印日志信息并且将该源 MAC 地址发送的 ARP 报文过滤掉；如果设置的检查模式为监控模式，则只打印日志信息，不会将该源 MAC 地址发送的 ARP 报文过滤掉。关于 ARP 日志信息功能的详细描述，请参见“网络互通配置指导”中的“ARP”。

如果 **undo arp source-mac** 命令中未指定检查模式，则关闭任意检查模式的源 MAC 地址固定的 ARP 攻击检测功能。

【举例】

开启源 MAC 地址固定的 ARP 攻击检测功能，并选择 **filter** 检查模式。

```
<Sysname> system-view
[Sysname] arp source-mac filter
```

1.3.2 arp source-mac aging-time

arp source-mac aging-time 命令用来配置源 MAC 地址固定的 ARP 攻击检测表项的老化时间。

undo arp source-mac aging-time 命令用来恢复缺省情况。

【命令】

arp source-mac aging-time *time*

undo arp source-mac aging-time

【缺省情况】

源 MAC 地址固定的 ARP 攻击检测表项的老化时间为 300 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

time：源 MAC 地址固定的 ARP 攻击检测表项的老化时间，取值范围为 60～6000，单位为秒。

【举例】

配置源 MAC 地址固定的 ARP 攻击检测表项的老化时间为 60 秒。

```
<Sysname> system-view
[Sysname] arp source-mac aging-time 60
```

1.3.3 arp source-mac exclude-mac

arp source-mac exclude-mac 命令用来配置保护 MAC 地址。当配置了保护 MAC 地址之后，即使该 ARP 报文中的 MAC 地址存在攻击也不会被检测过滤。

undo arp source-mac exclude-mac 命令用来取消配置的保护 MAC 地址。

【命令】

arp source-mac exclude-mac *mac-address*&<1-n>

undo arp source-mac exclude-mac [*mac-address*&<1-n>]

【缺省情况】

未配置任何保护 MAC 地址。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

mac-address&<1-n>：MAC 地址列表。其中，*mac-address* 表示配置的保护 MAC 地址，格式为 H-H-H。&<1-n>表示每次最多可以配置的保护 MAC 地址个数。n 的取值为 10。

【使用指导】

如果 **undo** 命令中未指定 MAC 地址，则取消所有已配置的保护 MAC 地址。

【举例】

配置源 MAC 地址固定的 ARP 攻击检查的保护 MAC 地址为 001e-1200-0213。

```
<Sysname> system-view
[Sysname] arp source-mac exclude-mac 001e-1200-0213
```

1.3.4 arp source-mac threshold

arp source-mac threshold 命令用来配置源 MAC 地址固定的 ARP 报文攻击检测阈值，当在固定的时间（5 秒）内收到源 MAC 地址固定的 ARP 报文超过该阈值则认为存在 ARP 报文攻击。

undo arp source-mac threshold 命令用来恢复缺省情况。

【命令】

arp source-mac threshold *threshold-value*

undo arp source-mac threshold

【缺省情况】

源 MAC 地址固定的 ARP 报文攻击检测阈值为 30。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

threshold-value：固定时间内源 MAC 地址固定的 ARP 报文攻击检测的阈值，单位为报文个数，取值范围为 1～5000。

【举例】

配置源 MAC 地址固定的 ARP 报文攻击检测阈值为 30 个。

```
<Sysname> system-view
[Sysname] arp source-mac threshold 30
```

1.3.5 display arp source-mac

display arp source-mac 命令用来显示检测到的源 MAC 地址固定的 ARP 攻击检测表项。

【命令】

display arp source-mac [**interface** *interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

interface *interface-type interface-number*：显示指定接口检测到的源 MAC 地址固定的 ARP 攻击检测表项，*interface-type interface-number* 表示指定接口的类型和编号。

【举例】

显示接口 GigabitEthernet1/0/1 检测到的源 MAC 地址固定的 ARP 攻击检测表项。

```
<Sysname> display arp source-mac interface gigabitethernet 1/0/1
Source-MAC          VLAN ID  Interface               Aging-time
23f3-1122-3344      4094     GE1/0/1                 10
```

表1-2 display arp source-mac 命令显示信息描述表

字段	描述
Source-MAC	检测到攻击的源MAC地址
VLAN ID	检测到攻击的VLAN ID
Interface	攻击来源的接口

字段	描述
Aging-time	ARP防攻击策略表项老化剩余时间，单位为秒

1.4 ARP报文源MAC地址一致性检查配置命令

1.4.1 arp valid-check enable

arp valid-check enable 命令用来开启 ARP 报文源 MAC 地址一致性检查功能。

undo arp valid-check enable 命令用来关闭 ARP 报文源 MAC 地址一致性检查功能。

【命令】

arp valid-check enable

undo arp valid-check enable

【缺省情况】

ARP 报文源 MAC 地址一致性检查功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

ARP 报文源 MAC 地址一致性检查功能主要应用于网关设备。

开启 ARP 报文源 MAC 地址一致性检查功能后，设备会对接收的 ARP 报文进行检查，如果以太网数据帧首部中的源 MAC 地址和 ARP 报文中的源 MAC 地址不同，则丢弃该报文。

【举例】

开启 ARP 报文源 MAC 地址一致性检查功能。

```
<Sysname> system-view
[Sysname] arp valid-check enable
```

1.5 ARP主动确认配置命令

1.5.1 arp active-ack enable

arp active-ack enable 命令用来开启 ARP 主动确认功能。

undo arp active-ack enable 命令用来关闭 ARP 主动确认功能。

【命令】

arp active-ack [**strict**] **enable**

undo arp active-ack [**strict**] **enable**

【缺省情况】

ARP 主动确认功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

strict：ARP 主动确认功能的严格模式。

【使用指导】

ARP 的主动确认功能主要应用于网关设备，防止攻击者仿冒用户欺骗网关设备。通过 **strict** 参数开启或关闭主动确认的严格模式。

【举例】

开启 ARP 主动确认功能。

```
<Sysname> system-view
[Sysname] arp active-ack enable
```

1.6 授权ARP配置命令

1.6.1 arp authorized enable

arp authorized enable 命令用来开启接口下的授权 ARP 功能。

undo arp authorized enable 命令用来关闭接口下的授权 ARP 功能。

【命令】

arp authorized enable

undo arp authorized enable

【缺省情况】

接口下的授权 ARP 功能处于关闭状态。

【视图】

VLAN 接口视图

【缺省用户角色】

network-admin

【举例】

开启 Vlan-interface200 接口下授权 ARP 功能。

```
<Sysname> system-view
[Sysname] interface vlan-interface 200
[Sysname-Vlan-interface200] arp authorized enable
```

1.7 ARP Detection配置命令

1.7.1 arp detection enable

arp detection enable 命令用来开启 ARP Detection 功能，即对 ARP 报文进行用户合法性检查。

undo arp detection enable 命令用来关闭 ARP Detection 功能。

【命令】

arp detection enable

undo arp detection enable

【缺省情况】

ARP Detection 功能处于关闭状态，即不进行用户合法性检查。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

【举例】

在 VLAN 2 下开启 ARP Detection 功能。

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] arp detection enable
```

【相关命令】

- **arp detection rule**

1.7.2 arp detection rule

arp detection rule 命令用来配置用户合法性检查规则。

undo arp detection rule 命令用来删除用户合法性检查规则。

【命令】

arp detection rule *rule-id* { **deny** | **permit** } **ip** { *ip-address* [*mask*] | **any** } **mac** { *mac-address* [*mask*] | **any** } [**vlan** *vlan-id*]

undo arp detection rule [*rule-id*]

【缺省情况】

未配置用户合法性检查规则。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

rule-id：用户合法性规则编号，取值范围为 0～511，数值越小表示该用户合法性规则优先级越高。

deny：丢弃指定范围内的 ARP 报文。

permit：转发指定范围内的 ARP 报文。

ip { *ip-address* [*mask*] | **any** }：指定报文的源 IP 地址范围。

- *ip-address*：表示报文的源 IP 地址，为点分十进制形式。
- *mask*：表示源 IP 地址的掩码，为点分十进制形式。如果未指定该参数，则 *ip-address* 表示主机地址。
- **any**：表示任意源 IP 地址。

mac { *mac-address* [*mask*] | **any** }：指定报文的源 MAC 地址范围。

- *mac-address*：表示报文的源 MAC 地址，格式为 H-H-H。
- *mask*：表示源 MAC 地址的掩码，格式为 H-H-H。如果未指定该参数，则 *mac-address* 表示主机 MAC 地址。
- **any**：表示任意源 MAC 地址。

vlan *vlan-id*：指定规则中匹配的 VLAN，*vlan-id* 的取值范围为 1～4094。如果未指定该参数，则不对报文中的 VLAN 进行匹配检查。

【使用指导】

只有配置了 **arp detection enable** 命令后，通过命令 **arp detection rule** 配置的规则才生效。

使用 **undo arp detection rule** 命令时，如果未指定 *rule-id*，则会删除设备上所有已配置的用户合法性规则。

【举例】

配置用户合法性规则，规则编号为 0，规则内容为转发源地址为 10.1.1.1，掩码为 255.255.0.0，源 MAC 地址为 0001-0203-0405，掩码为 ffff-ffff-0000 的 ARP 报文。并在 VLAN2 中开启用户合法性检查功能。

```
<Sysname> system-view
[Sysname] arp detection rule 0 permit ip 10.1.1.1 255.255.0.0 mac 0001-0203-0405
ffff-ffff-0000
[Sysname] vlan 2
[Sysname-vlan2] arp detection enable
```

【相关命令】

- **arp detection enable**

1.7.3 arp detection trust

arp detection trust 命令用来配置接口为 ARP 信任接口。

undo arp detection trust 命令用来恢复缺省情况。

【命令】

arp detection trust

undo arp detection trust

【缺省情况】

接口为 ARP 非信任接口。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【举例】

配置二层以太网接口 GigabitEthernet1/0/1 为 ARP 信任接口。

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

1.7.4 arp detection validate

arp detection validate 命令用来开启对 ARP 报文的目的 MAC 地址或源 MAC 地址、IP 地址的有效性检查。

undo arp detection validate 命令用来关闭对 ARP 报文的有效性检查。

【命令】

arp detection validate { **dst-mac** | **ip** | **src-mac** } *

undo arp detection validate [**dst-mac** | **ip** | **src-mac**] *

【缺省情况】

ARP 报文有效性检查功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

dst-mac：检查 ARP 应答报文中的目的 MAC 地址，是否为全 0 或者全 1，是否和以太网报文头中的目的 MAC 地址一致。全 0、全 1、不一致的报文都是无效的，无效的报文需要被丢弃。

ip：检查 ARP 报文源 IP 和目的 IP 地址，全 1 或者组播 IP 地址都是不合法的，需要丢弃。对于 ARP 应答报文，源 IP 和目的 IP 地址都进行检查；对于 ARP 请求报文，只检查源 IP 地址。

src-mac：检查 ARP 报文中的源 MAC 地址和以太网报文头中的源 MAC 地址是否一致，一致认为有效，否则丢弃。

【使用指导】

开启有效性检查时可以指定某一种检查方式也可以配置成多种检查方式的组合。

关闭时可以指定关闭某一种或多种检查，在不指定检查方式时，表示关闭所有有效性检查。

【举例】

开启对 ARP 报文的 MAC 地址和 IP 地址的有效性检查。

```
<Sysname> system-view
[Sysname] arp detection validate dst-mac ip src-mac
```

1.7.5 arp restricted-forwarding enable

arp restricted-forwarding enable 命令用来开启 ARP 报文强制转发功能。

undo arp restricted-forwarding enable 命令用来关闭 ARP 报文强制转发功能。

【命令】

arp restricted-forwarding enable

undo arp restricted-forwarding enable

【缺省情况】

ARP 报文强制转发功能处于关闭状态。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

【举例】

开启 VLAN 2 的 ARP 报文强制转发功能。

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] arp restricted-forwarding enable
```

1.7.6 display arp detection

display arp detection 命令用来显示配置了 ARP Detection 功能的 VLAN。

【命令】

display arp detection

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【举例】

显示所有配置了 ARP Detection 功能的 VLAN。

```
<Sysname> display arp detection
 ARP detection is enabled in the following VLANs:
 1-2, 4-5
```

表1-3 display arp detection 命令显示信息描述表

字段	描述
ARP detection is enabled in the following VLANs	配置了ARP Detection功能的VLAN信息，如果不存在配置了ARP Detection功能的VLAN，则显示“ARP detection is not enabled in any VLAN.”

【相关命令】

- **arp detection enable**

1.7.7 display arp detection statistics

display arp detection statistics 命令用来显示 ARP Detection 丢弃报文的统计信息。

【命令】

display arp detection statistics [**interface** *interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

interface *interface-type interface-number*：显示指定接口的 ARP Detection 丢弃报文的统计信息。*interface-type interface-number* 用来指定接口类型和编号。如果未指定本参数，则显示所有接口的 ARP Detection 丢弃报文的统计信息。

【使用指导】

按接口显示用户合法性检查和报文有效性检查的统计情况，只显示 ARP Detection 功能报文的丢弃情况。

【举例】

显示 ARP Detection 丢弃报文的统计信息。

```
<Sysname> display arp detection statistics
State: U-Untrusted  T-Trusted
ARP packets dropped by ARP inspect checking:
Interface(State)            IP        Src-MAC   Dst-MAC   Inspect
GE1/0/1(U)                  40        0         0         78
GE1/0/2(U)                  0         0         0         0
```

表1-4 display arp detection statistics 命令显示信息描述表

字段	描述
State	接口状态： • U：ARP 非信任接口 • T：ARP 信任接口
Interface(State)	ARP报文入接口，State表示该接口的信任状态
IP	ARP报文源和目的IP地址检查不通过丢弃的报文计数
Src-MAC	ARP报文源MAC地址检查不通过丢弃的报文计数
Dst-MAC	ARP报文目的MAC地址检查不通过丢弃的报文计数
Inspect	ARP报文结合用户合法性检查不通过丢弃的报文计数

【相关命令】

- **reset arp detection statistics**

1.7.8 reset arp detection statistics

reset arp detection statistics 命令用来清除 ARP Detection 的报文丢弃统计信息。

【命令】

reset arp detection statistics [**interface** *interface-type interface-number*]

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface *interface-type interface-number*：表示清除指定接口下的 ARP Detection 的报文丢弃统计信息。*interface-type interface-number* 用来指定接口类型和编号。如果未指定本参数，则清除所有接口下的 ARP Detection 报文丢弃统计信息。

【举例】

清除所有的 ARP Detection 的报文丢弃统计信息。

```
<Sysname> reset arp detection statistics
```

【相关命令】

- **display arp detection statistics**

1.8 ARP自动扫描、固化配置命令

1.8.1 arp fixup

arp fixup 命令用来将设备上的动态 ARP 表项转化成静态 ARP 表项。

【命令】

arp fixup

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

本命令将当前的动态 ARP 表项转换为静态 ARP 表项，后续学习到的动态 ARP 表项可以通过再次执行 **arp fixup** 命令进行固化。

固化后的静态 ARP 表项与配置产生的静态 ARP 表项相同。

固化生成的静态 ARP 表项数量同样受到设备可以支持的静态 ARP 表项数目的限制，由于静态 ARP 表项数量的限制可能导致只有部分动态 ARP 表项被固化。

如果用户执行固化前有 D 个动态 ARP 表项，S 个静态 ARP 表项，由于固化过程中存在动态 ARP 表项的老化或者新建动态 ARP 表项的情况，所以固化后的静态 ARP 表项可能为（D＋S＋M－N）个。其中，M 为固化过程中新建的动态 ARP 表项个数，N 为固化过程中老化的动态 ARP 表项个数。

通过固化生成的静态 ARP 表项，可以通过命令行 **undo arp** *ip-address* 逐条删除，也可以通过命令行 **reset arp all** 或 **reset arp static** 全部删除。

【举例】

将设备上的动态 ARP 表项转化成静态 ARP 表项。

```
<Sysname> system-view
[Sysname] arp fixup
```

1.8.2 arp scan

arp scan 命令用来开启 ARP 自动扫描功能。

【命令】

arp scan [*start-ip-address* **to** *end-ip-address*]

【视图】

VLAN 接口视图

【缺省用户角色】

network-admin

【参数】

start-ip-address：ARP 扫描区间的起始 IP 地址。起始 IP 地址必须小于等于终止 IP 地址。

end-ip-address：ARP 扫描区间的终止 IP 地址。

【使用指导】

ARP 自动扫描功能可以对接口下指定地址范围内的邻居进行扫描，对于已存在 ARP 表项的 IP 地址不进行扫描。

如果用户知道局域网内邻居分配的 IP 地址范围，指定了 ARP 扫描区间，则对该范围内的邻居进行扫描，减少扫描等待的时间。如果指定的扫描区间同时在接口下多个 IP 地址的网段内，则发送的 ARP 请求报文的源 IP 地址选择网段范围较小的接口 IP 地址。

如果用户不指定 ARP 扫描区间的起始 IP 地址和终止 IP 地址，则仅对接口下的主 IP 地址网段内的邻居进行扫描。其中，发送的 ARP 请求报文的源 IP 地址就是接口的主 IP 地址。

ARP 扫描区间的起始 IP 地址和终止 IP 地址必须与接口的 IP 地址（主 IP 地址或手工配置的从 IP 地址）在同一网段。

扫描操作可能比较耗时，用户可以通过<Ctrl_C>来终止扫描（在终止扫描时，对于已经收到的邻居应答，会建立该邻居的动态 ARP 表项）。

【举例】

对接口 Vlan-interface2 下的主 IP 地址网段内的邻居进行扫描。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp scan
```

对接口 Vlan-interface2 下指定地址范围内的邻居进行扫描。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp scan 1.1.1.1 to 1.1.1.20
```

目 录

1 SSL

1.1 SSL配置命令

1.1.1 display ssl client-policy

display ssl client-policy 命令用来显示 SSL 客户端策略的信息。

【命令】

display ssl client-policy [*policy-name*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

policy-name：显示指定的 SSL 客户端策略的信息，为 1～31 个字符的字符串，不区分大小写。如果不指定本参数，则显示所有 SSL 客户端策略的信息。

【举例】

显示名为 policy1 的 SSL 客户端策略的信息。

```
<Sysname> display ssl client-policy policy1
 SSL client policy: policy1
     SSL version: SSL 3.0
     PKI domain: client-domain
     Preferred ciphersuite:
         RSA_AES_128_CBC_SHA
     Server-verify: enabled
```

表1-1 display ssl client-policy 命令显示信息描述表

字段	描述
SSL client policy	SSL客户端策略名
SSL version	SSL客户端策略使用的SSL协议版本
PKI domain	SSL客户端策略使用的PKI域
Preferred ciphersuite	SSL客户端策略支持的加密套件
Server-verify	（暂不支持）SSL客户端策略的服务器端验证模式，取值包括： • disabled：不要求对 SSL 服务器进行基于数字证书的身份验证 • enabled：要求对 SSL 服务器进行基于数字证书的身份验证

1.1.2 pki-domain (SSL client policy view)

pki-domain 命令用来配置 SSL 客户端策略所使用的 PKI 域。

undo pki-domain 命令用来恢复缺省情况。

【命令】

pki-domain *domain-name*

undo pki-domain

【缺省情况】

未指定 SSL 客户端策略所使用的 PKI 域。

【视图】

SSL 客户端策略视图

【缺省用户角色】

network-admin

【参数】

domain-name：PKI 域的域名，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

如果通过本命令指定了 SSL 客户端策略使用的 PKI 域，则引用该客户端策略的 SSL 客户端将通过该 PKI 域获取客户端的数字证书。

【举例】

配置 SSL 客户端策略所使用的 PKI 域为 client-domain。

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] pki-domain client-domain
```

【相关命令】

- **display ssl client-policy**

1.1.3 prefer-cipher

prefer-cipher 命令用来配置 SSL 客户端策略支持的加密套件。

undo prefer-cipher 命令用来恢复缺省情况。

【命令】

prefer-cipher { dhe_rsa_aes_128_cbc_sha | dhe_rsa_aes_128_cbc_sha256 | dhe_rsa_aes_256_cbc_sha | dhe_rsa_aes_256_cbc_sha256 | ecdhe_ecdsa_aes_128_cbc_sha256 | ecdhe_ecdsa_aes_128_gcm_sha256 | ecdhe_ecdsa_aes_256_cbc_sha384 | ecdhe_ecdsa_aes_256_gcm_sha384 | ecdhe_rsa_aes_128_cbc_sha256 | ecdhe_rsa_aes_128_gcm_sha256 | ecdhe_rsa_aes_256_cbc_sha384 | ecdhe_rsa_aes_256_gcm_sha384 | exp_rsa_des_cbc_sha | exp_rsa_rc2_md5 | exp_rsa_rc4_md5 | rsa_3des_ede_cbc_sha | rsa_aes_128_cbc_sha | rsa_aes_128_cbc_sha256 |

rsa_aes_256_cbc_sha | rsa_aes_256_cbc_sha256 | rsa_des_cbc_sha | rsa_rc4_128_md5 | rsa_rc4_128_sha } *

undo prefer-cipher

【缺省情况】

SSL 客户端策略支持的加密套件为 **dhe_rsa_aes_128_cbc_sha**、**dhe_rsa_aes_256_cbc_sha**、**rsa_3des_ede_cbc_sha**、**rsa_aes_128_cbc_sha**、**rsa_aes_256_cbc_sha**。

【视图】

SSL 客户端策略视图

【缺省用户角色】

network-admin

【参数】

dhe_rsa_aes_128_cbc_sha：密钥交换算法采用 DHE RSA、数据加密算法采用 128 位的 AES、MAC 算法采用 SHA。

dhe_rsa_aes_128_cbc_sha256：密钥交换算法采用 DHE RSA、数据加密算法采用 128 位的 AES_CBC、MAC 算法采用 SHA256。

dhe_rsa_aes_256_cbc_sha：密钥交换算法采用 DHE RSA、数据加密算法采用 256 位的 AES、MAC 算法采用 SHA。

dhe_rsa_aes_256_cbc_sha256：密钥交换算法采用 DHE RSA、数据加密算法采用 256 位的 AES_CBC、MAC 算法采用 SHA256。

ecdhe_ecdsa_aes_128_cbc_sha256：密钥交换算法采用 ECDHE ECDSA、数据加密算法采用 128 位的 AES_CBC、MAC 算法采用 SHA256。

ecdhe_ecdsa_aes_128_gcm_sha256：密钥交换算法采用 ECDHE ECDSA、数据加密算法采用 128 位的 AES_GCM、MAC 算法采用 SHA256。

ecdhe_ecdsa_aes_256_cbc_sha384：密钥交换算法采用 ECDHE ECDSA、数据加密算法采用 256 位的 AES_CBC、MAC 算法采用 SHA384。

ecdhe_ecdsa_aes_256_gcm_sha384：密钥交换算法采用 ECDHE ECDSA、数据加密算法采用 256 位的 AES_GCM、MAC 算法采用 SHA384。

ecdhe_rsa_aes_128_cbc_sha256：密钥交换算法采用 ECDHE RSA、数据加密算法采用 128 位的 AES_CBC、MAC 算法采用 SHA256。

ecdhe_rsa_aes_128_gcm_sha256：密钥交换算法采用 ECDHE RSA、数据加密算法采用 128 位的 AES_GCM、MAC 算法采用 SHA256。

ecdhe_rsa_aes_256_cbc_sha384：密钥交换算法采用 ECDHE RSA、数据加密算法采用 256 位的 AES_CBC、MAC 算法采用 SHA384。

ecdhe_rsa_aes_256_gcm_sha384：密钥交换算法采用 ECDHE RSA、数据加密算法采用 256 位的 AES_GCM、MAC 算法采用 SHA384。

exp_rsa_des_cbc_sha：满足出口限制的算法套件。密钥交换算法采用 RSA、数据加密算法采用 DES_CBC、MAC 算法采用 SHA。

exp_rsa_rc2_md5：满足出口限制的算法套件。密钥交换算法采用 RSA、数据加密算法采用 RC2、MAC 算法采用 MD5。

exp_rsa_rc4_md5：满足出口限制的算法套件。密钥交换算法采用 RSA、数据加密算法采用 RC4、MAC 算法采用 MD5。

rsa_3des_ede_cbc_sha：密钥交换算法采用 RSA、数据加密算法采用 3DES_EDE_CBC、MAC 算法采用 SHA。

rsa_aes_128_cbc_sha：密钥交换算法采用 RSA、数据加密算法采用 128 位 AES_CBC、MAC 算法采用 SHA。

rsa_aes_128_cbc_sha256：密钥交换算法采用 RSA、数据加密算法采用 128 位的 AES_CBC、MAC 算法采用 SHA256。

rsa_aes_256_cbc_sha：密钥交换算法采用 RSA、数据加密算法采用 256 位 AES_CBC、MAC 算法采用 SHA。

rsa_aes_256_cbc_sha256：密钥交换算法采用 RSA、数据加密算法采用 256 位的 AES_CBC、MAC 算法采用 SHA256。

rsa_des_cbc_sha：密钥交换算法采用 RSA、数据加密算法采用 DES_CBC、MAC 算法采用 SHA。

rsa_rc4_128_md5：密钥交换算法采用 RSA、数据加密算法采用 128 位的 RC4、MAC 算法采用 MD5。

rsa_rc4_128_sha：密钥交换算法采用 RSA、数据加密算法采用 128 位的 RC4、MAC 算法采用 SHA。

【使用指导】

为了提高安全性，SSL 协议采用了如下算法：

- 数据加密算法：用来对传输的数据进行加密，以保证数据传输的私密性。常用的数据加密算法通常为对称密钥算法。使用对称密钥算法时，要求 SSL 服务器端和 SSL 客户端具有相同的密钥。
- MAC（Message Authentication Code，消息验证码）算法：用来计算数据的 MAC 值，以防止发送的数据被篡改。常用的 MAC 算法有 MD5、SHA 等。使用 MAC 算法时，要求 SSL 服务器端和 SSL 客户端具有相同的密钥。
- 密钥交换算法：用来实现密钥交换，以保证对称密钥算法、MAC 算法中使用的密钥在 SSL 服务器端和 SSL 客户端之间安全地传递。常用的密钥交换算法通常为非对称密钥算法，如 RSA。

通过本命令可以配置 SSL 客户端策略支持的算法组合。例如，**rsa_des_cbc_sha** 表示 SSL 客户端支持的密钥交换算法为 RSA、数据加密算法为 DES_CBC、MAC 算法为 SHA。

SSL 客户端将本端支持的加密套件发送给 SSL 服务器，SSL 服务器将自己支持的加密套件与 SSL 客户端支持的加密套件比较。如果 SSL 服务器支持的加密套件中存在 SSL 客户端支持的加密套件，则加密套件协商成功；否则，加密套件协商失败。

多次执行本命令，最后一次执行的命令生效。

【举例】

配置 SSL 客户端策略支持的加密套件为：密钥交换算法采用 RSA、数据加密算法采用 128 位 AES_CBC、MAC 算法采用 SHA。

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
```

```
[Sysname-ssl-client-policy-policy1] prefer-cipher rsa_aes_128_cbc_sha
```

【相关命令】

- **display ssl client-policy**

1.1.4 ssl client-policy

ssl client-policy 命令用来创建 SSL 客户端策略，并进入 SSL 客户端策略视图。如果指定的 SSL 客户端策略已经存在，则直接进入 SSL 客户端策略视图。

undo ssl client-policy 命令用来删除指定的 SSL 客户端策略。

【命令】

ssl client-policy *policy-name*

undo ssl client-policy *policy-name*

【缺省情况】

不存在 SSL 客户端策略。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

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

【使用指导】

SSL 客户端策略视图下可以配置 SSL 客户端启动时使用的 SSL 参数，如使用的 PKI 域、支持的加密套件等。只有与应用层协议，如 DDNS（Dynamic Domain Name System，动态域名系统），关联后，SSL 客户端策略才能生效。

【举例】

创建 SSL 客户端策略 policy1，并进入 SSL 客户端策略视图。

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1]
```

【相关命令】

- **display ssl client-policy**

1.1.5 version

version 命令用来配置 SSL 客户端策略使用的 SSL 协议版本。

undo version 命令恢复缺省情况。

【命令】

version { **ssl3.0** | **tls1.0** | **tls1.1** | **tls1.2** }

undo version

【缺省情况】

SSL 客户端策略使用的 SSL 协议版本为 TLS 1.0。

【视图】

SSL 客户端策略视图

【缺省用户角色】

network-admin

【参数】

ssl3.0：SSL 客户端策略使用的 SSL 协议版本为 SSL 3.0。

tls1.0：SSL 客户端策略使用的 SSL 协议版本为 TLS 1.0。

tls1.1：SSL 客户端策略使用的 SSL 协议版本为 TLS1.1。

tls1.2：SSL 客户端策略使用的 SSL 协议版本为 TLS1.2。

【使用指导】

对安全性要求较高的环境下，建议为不要为 SSL 客户端指定 SSL3.0 版本。

多次执行本命令，最后一次执行的命令生效。

【举例】

配置 SSL 客户端策略使用的 SSL 协议版本为 TLS 1.0。

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] version tls1.0
```

【相关命令】

- **display ssl client-policy**