目 录

1 ACL 配置

说明

- 本文将用于 IPv4 和 IPv6 的 ACL 分别简称为 IPv4 ACL 和 IPv6 ACL。若非特别指明，本文所指的 ACL 均包括 IPv4 ACL 和 IPv6 ACL。
- 本章中提到的三层以太网端口是指工作模式被配置成三层模式的以太网端口，有关以太网端口工作模式切换的操作，请参见“二层技术-以太网交换配置指导”中的“以太网端口配置”部分。

1.1 ACL 简介

1.1.1 ACL 概述

ACL（Access Control List，访问控制列表）是用来实现流识别功能的。网络设备为了过滤报文，需要配置一系列的匹配条件对报文进行分类，这些条件可以是报文的源地址、目的地址、端口号等。

当设备的端口接收到报文后，即根据当前端口上应用的 ACL 规则对报文的字段进行分析，在识别出特定的报文之后，根据预先设定的策略允许或禁止该报文通过。

由 ACL 定义的报文匹配规则，可以被其它需要对流量进行区分的场合引用，如包过滤、QoS 中流分类规则的定义等。

1.1.2 ACL 在交换机上的应用方式

当 ACL 被其他功能引用时，根据设备在实现该功能时的处理方式（硬件处理或者软件处理），ACL 可以被分为基于硬件的应用和基于软件的应用。

典型的基于硬件的应用包括：包过滤、QoS 策略；基于软件的应用包括：路由、对登录用户（Telnet、SNMP、WEB）进行控制等。

在某些应用方式下，例如 QoS 策略中，ACL 仅用于匹配报文，ACL 规则中的动作（**deny** 或 **permit**）被忽略，不作为对报文进行丢弃或转发的依据，类似情况请参见相应功能中的说明。

说明

- 当 ACL 被 QoS 策略引用进行流分类时，如果报文没有与 ACL 中的规则匹配，此时交换机不会使用流行为中定义的动作对此类报文进行处理。
- 当 ACL 被用于对 Telnet、SNMP 和 WEB 登录用户进行控制时，如果报文没有与 ACL 中的规则匹配，此时交换机对此类报文采取的动作为 deny，即拒绝报文通过。
- 关于应用ACL对报文进行过滤的介绍和配置，请参见 应用ACL进行报文过滤。

1.1.3 ACL 的分类

根据功能以及规则制订依据的不同，可以将ACL分为三种类型，如 表 1-1所示。

表1-1 ACL 的分类

ACL 类型	编号范围	适用的 IP 版本	规则制订依据
基本 ACL	2000～2999	IPv4	只根据报文的源 IP 地址信息制定匹配规则
		IPv6	只根据报文的源 IPv6 地址信息制定匹配规则
高级 ACL	3000～3999	IPv4	根据报文的源 IP 地址信息、目的 IP 地址信息、IP 承载的协议类型、协议的特性等三、四层信息制定匹配规则
		IPv6	根据报文的源 IPv6 地址信息、目的 IPv6 地址信息、IPv6 承载的协议类型、协议的特性等三、四层信息制定匹配规则
二层 ACL	4000～4999	IPv4&IPv6	根据报文的源 MAC 地址、目的 MAC 地址、802.1p 优先级、二层协议类型等二层信息制定匹配规则

1.1.4 ACL 的编号和名称

用户在创建 ACL 时必须为其指定编号，系统将根据用户所指定的编号来创建不同类型的 ACL。

通常名称比编号更易于记忆和识别，因此用户在创建 ACL 时，还可以选择是否为其指定名称，而且只能在创建 ACL 时为其指定名称。ACL 一旦创建，便不允许对其名称进行修改或删除。

当 ACL 创建完成后，用户可以通过指定编号或名称的方式来指定该 ACL，以便对其进行操作。

说明

二层 ACL 的编号和名称全局唯一；IPv4 基本和高级 ACL 的编号和名称只在 IPv4 中唯一；IPv6 基本和高级 ACL 的编号和名称也只在 IPv6 中唯一。

1.1.5 ACL 的匹配顺序

一个 ACL 由一条或多条描述报文匹配选项的判断语句组成，这样的判断语句就称为“规则”。由于每条规则中的报文匹配选项不同，从而使这些规则之间可能存在重复甚至矛盾的地方，因此在将一个报文与 ACL 的各条规则进行匹配时，就需要有明确的匹配顺序来确定规则执行的优先级。ACL 的规则匹配顺序有以下两种：

- 配置顺序：按照用户配置规则的先后顺序进行匹配，但由于本质上系统是按照规则编号由小到大进行匹配，因此后插入的规则如果编号较小也有可能先被匹配。
- 自动排序：按照“深度优先”原则由深到浅进行匹配，不同类型ACL的“深度优先”排序法则如 表 1-2所示。

说明

当报文与各条规则进行匹配时，一旦匹配上某条规则，就不会再继续匹配下去，系统将依据该规则对该报文执行相应的操作。

表1-2 各类型 ACL 的“深度优先”排序法则

ACL 类型	“深度优先”排序法则
IPv4 基本 ACL	(1) 先看规则中是否携带有 VPN 实例，携带 VPN 实例者优先 (2) 如果 VPN 实例的携带情况相同，再比较源 IPv4 地址范围，范围较小者优先 (3) 如果源 IP 地址范围也相同，再比较配置顺序，配置在前者优先
IPv4 高级 ACL	(1) 先看规则中是否携带有 VPN 实例，携带 VPN 实例者优先 (2) 如果 VPN 实例的携带情况相同，再比较协议范围，指定有 IPv4 承载的协议类型者优先 (3) 如果协议范围也相同，再比较源 IPv4 地址范围，较小者优先 (4) 如果源 IPv4 地址范围也相同，再比较目的 IPv4 地址范围，较小者优先 (5) 如果目的 IPv4 地址范围也相同，再比较四层端口（即 TCP/UDP 端口）号范围，较小者优先 (6) 如果四层端口号范围也相同，再比较配置顺序，配置在前者优先
IPv6 基本 ACL	(1) 先比较源 IPv6 地址范围，较小者优先 (2) 如果源 IPv6 地址范围相同，再比较配置顺序，配置在前者优先
IPv6 高级 ACL	(1) 先比较协议范围，指定有 IPv6 承载的协议类型者优先 (2) 如果协议范围相同，再比较源 IPv6 地址范围，较小者优先 (3) 如果源 IPv6 地址范围也相同，再比较目的 IPv6 地址范围，较小者优先 (4) 如果目的 IPv6 地址范围也相同，再比较四层端口（即 TCP/UDP 端口）号范围，较小者优先 (5) 如果四层端口号范围也相同，再比较配置顺序，配置在前者优先
二层 ACL	(1) 先比较源 MAC 地址范围，较小者优先 (2) 如果源 MAC 地址范围相同，再比较目的 MAC 地址范围，较小者优先 (3) 如果目的 MAC 地址范围也相同，再比较配置顺序，配置在前者优先

说明

- 比较 IPv4 地址范围的大小，就是比较 IPv4 地址通配符掩码中“0”位的多少：“0”位越多，范围越小。通配符掩码（又称反向掩码）以点分十进制表示，并以二进制的“0”表示“匹配”，“1”表示“不关心”，这与子网掩码恰好相反，譬如子网掩码 255.255.255.0 对应的通配符掩码就是 0.0.0.255。此外，通配符掩码中的“0”或“1”都可以是不连续的，这样可以更加灵活地进行匹配，譬如 0.255.0.255 就是一个合法的通配符掩码。
- 比较 IPv6 地址范围的大小，就是比较 IPv6 地址前缀的长短：前缀越长，范围越小。
- 比较 MAC 地址范围的大小，就是比较 MAC 地址掩码中“1”位的多少：“1”位越多，范围越小。

1.1.6 ACL 的步长

ACL 内的每条规则都有自己的编号，每个规则的编号在一个 ACL 中都是唯一的。在创建规则时，可以人为地为其指定一个编号，也可以由系统为其自动分配一个编号。

在自动分配编号时，为了方便后续在已有规则之前插入新的规则，系统通常会在相邻编号之间留下一定的空间，这个空间的大小（即相邻编号之间的差值）就称为 ACL 的步长。譬如，当步长为 5 时，系统会将编号 0、5、10、15……依次分配给新创建的规则。

系统为规则自动分配编号的方式如下：系统按照步长从 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。

说明

如果改变步长，ACL 内原有全部规则的编号都将自动从 0 开始按新步长重新排列。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。

1.1.7 ACL 的生效时间段

时间段用于描述一个特定的时间范围。用户可能有这样的需求：一些 ACL 规则只需在某个或某些特定的时间段内生效（即进行报文过滤），这也称为基于时间段的 ACL 过滤。为此，用户可以先配置一个或多个时间段，然后在 ACL 规则下引用这些时间段，那么该规则将只在指定的时间段内生效。此外，如果某 ACL 规则所引用的时间段尚未配置，系统将给出提示信息，并仍允许该规则成功创建，但该规则将不会在其引用的时间段完成配置前生效。

1.1.8 ACL 对 IPv4 分片报文的处理

传统的报文过滤并不处理所有的 IPv4 报文分片，而只对首片分片报文进行匹配处理，而对后续分片一律放行。这样，网络攻击者可能构造后续的分片报文进行流量攻击，就带来了安全隐患。

为提高网络安全性，缺省情况下 ACL 规则会对非分片报文及分片报文中的每一片都进行匹配。为提高匹配效率，也可以通过使用 **fragment** 参数，来标识该 ACL 规则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。

1.2 ACL 配置任务简介

表1-3 ACL 配置任务简介

配置任务	说明	详细配置
配置 ACL 的生效时间段	可选	1.3.1
配置 IPv4 基本 ACL	至少选其一	1.3.2 1.
配置 IPv6 基本 ACL		1.3.2 2.
配置 IPv4 高级 ACL		1.3.3 1.
配置 IPv6 高级 ACL		1.3.3 2.
配置二层 ACL		1.3.4
配置 ACL 规则注释信息	可选	1.3.5
复制 ACL	可选	1.3.6
应用 ACL 进行报文过滤	可选	1.3.7

1.3 配置 ACL

1.3.1 配置 ACL 的生效时间段

时间段可分为以下两种：

- 周期时间段：该时间段以一周为周期循环生效。
- 绝对时间段：该时间段在指定时间范围内生效。

表1-4 配置 ACL 的生效时间段

操作	命令	说明
进入系统视图	**system-view**	-
创建时间段	**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* }	必选 缺省情况下，不存在任何时间段

说明

- 使用同一名称可以配置多条不同的时间段，以达到这样的效果：各周期时间段之间以及各绝对时间段之间分别取并集之后，再取二者的交集作为最终生效的时间范围。
- 最多可以创建 256 个不同名称的时间段，而同一名称下最多可以配置 32 条周期时间段和 12 条绝对时间段。

1.3.2 配置基本 ACL

1. 配置 IPv4 基本 ACL

IPv4 基本 ACL 只根据报文的源 IP 地址信息制定匹配规则，对 IPv4 报文进行相应的分析处理。

表1-5 配置 IPv4 基本 ACL

操作	命令	说明
进入系统视图	**system-view**	-
创建 IPv4 基本 ACL，并进入 IPv4 基本 ACL 视图	**acl number** *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]	必选 缺省情况下，不存在任何 ACL IPv4 基本 ACL 的编号范围为 2000～2999
配置 ACL 的描述信息	**description** *text*	可选 缺省情况下，ACL 没有任何描述信息
配置规则编号的步长	**step** *step-value*	可选 缺省情况下，规则编号的步长为 5

操作	命令	说明
创建规则	**rule** [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **source** { *sour-addr sour-wildcard* | **any** } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *	必选 缺省情况下，IPv4 基本 ACL 内不存在任何规则 重复执行本命令可以创建多条规则 需要注意的是，当 IPv4 基本 ACL 被 QoS 策略引用对报文进行流分类时，不支持配置 **vpn-instance** 参数，在规则中配置的 **logging** 和 **counting** 参数不会生效
配置规则的描述信息	**rule** *rule-id* **comment** *text*	可选 缺省情况下，规则没有任何描述信息
开启基于硬件应用的 ACL 统计功能	**hardware-count enable**	可选 该功能用于统计 ACL 在硬件应用时被匹配成功的次数 缺省情况下，基于硬件应用的 ACL 统计功能处于关闭状态 当 ACL 被 QoS 策略引用对报文进行流分类时，本功能不会生效

说明

如果在创建 IPv4 基本 ACL 时为其指定了名称，则也可以使用 **acl name** *acl-name* 命令通过指定名称的方式进入其视图。

2. 配置 IPv6 基本 ACL

IPv6 基本 ACL 只根据报文的源 IPv6 地址信息制定匹配规则，对 IPv6 报文进行相应的分析处理。

表1-6 配置 IPv6 基本 ACL

操作	命令	说明
进入系统视图	**system-view**	-
创建 IPv6 基本 ACL，并进入 IPv6 基本 ACL 视图	**acl ipv6 number** *acl6-number* [**name** *acl6-name*] [**match-order** { **auto** | **config** }]	必选 缺省情况下，不存在任何 ACL IPv6 基本 ACL 的编号范围为 2000～2999
配置 ACL 的描述信息	**description** *text*	可选 缺省情况下，ACL 没有任何描述信息
配置规则编号的步长	**step** *step-value*	可选 缺省情况下，规则编号的步长为 5

操作	命令	说明
创建规则	**rule** [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **source** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* | **any** } | **time-range** *time-range-name*] *	必选 缺省情况下，IPv6 基本 ACL 内不存在任何规则 重复执行本命令可以创建多条规则 需要注意的是，当 IPv6 基本 ACL 被 QoS 策略引用对报文进行流分类时，不支持配置 **fragment** 参数，在规则中配置的 **logging** 和 **counting** 参数不会生效
配置规则的描述信息	**rule** *rule-id* **comment** *text*	可选 缺省情况下，规则没有任何描述信息
开启基于硬件应用的 ACL 统计功能	**hardware-count enable**	可选 该功能用于统计 ACL 在硬件应用时被匹配成功的次数 缺省情况下，基于硬件应用的 ACL 统计功能处于关闭状态 当 ACL 被 QoS 策略引用对报文进行流分类时，本功能不会生效

说明

如果在创建 IPv6 基本 ACL 时为其指定了名称，则也可以使用 **acl ipv6 name** *acl6-name* 命令通过指定名称的方式进入其视图。

1.3.3 配置高级 ACL

1. 配置 IPv4 高级 ACL

IPv4 高级 ACL 可以使用报文的源 IPv4 地址信息、目的 IPv4 地址信息、IPv4 承载的协议类型、协议的特性（例如 TCP 或 UDP 的源端口、目的端口，TCP 标记，ICMP 协议的消息类型、消息码等）等信息来制定匹配规则。IPv4 高级 ACL 支持对以下三种报文优先级进行分析处理：

- ToS（Type of Service，服务类型）优先级；
- IP 优先级；
- DSCP（Differentiated Services Codepoint，差分服务编码点）优先级。

用户可以利用 IPv4 高级 ACL 定义比 IPv4 基本 ACL 更准确、丰富、灵活的匹配规则。

表1-7 配置 IPv4 高级 ACL

操作	命令	说明
进入系统视图	**system-view**	-
创建 IPv4 高级 ACL，并进入 IPv4 高级 ACL 视图	**acl number** *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]	必选 缺省情况下，不存在任何 ACL IPv4 高级 ACL 的编号范围为 3000～3999

操作	命令	说明
配置 ACL 的描述信息	**description** *text*	可选 缺省情况下，ACL 没有任何描述信息
配置规则编号的步长	**step** *step-value*	可选 缺省情况下，规则编号的步长为 5
创建规则	**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-addr dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | **dscp** *dscp* | **fragment** | **icmp-type** { *icmp-type icmp-code* | *icmp-message* } | **logging** | **precedence** *precedence* | **reflective** | **source** { *sour-addr sour-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name* | **tos** *tos* | **vpn-instance** *vpn-instance-name*] *	必选 缺省情况下，IPv4 高级 ACL 内不存在任何规则 目前不支持 **reflective** 参数 重复执行本命令可以创建多条规则 目前暂不支持配置 **reflective** 参数 需要注意的是，当 IPv4 高级 ACL 被 QoS 策略引用对报文进行流分类时： • 不支持配置 **vpn-instance** 参数 • 在规则中配置的 **logging** 和 **counting** 参数不会生效 • 不支持配置操作符 *operator* 取值为 **neq** 当 IPv4 高级 ACL 用于包过滤功能时，不支持配置操作符 *operator* 取值为 **neq**
配置规则的描述信息	**rule** *rule-id* **comment** *text*	可选 缺省情况下，规则没有任何描述信息
使能基于硬件应用的 ACL 规则匹配统计功能	**hardware-count enable**	可选 缺省情况下，基于硬件应用的 ACL 规则匹配统计功能处于关闭状态 当 ACL 被 QoS 策略引用对报文进行流分类时，本功能不会生效

说明

如果在创建 IPv4 高级 ACL 时为其指定了名称，则也可以使用 **acl name** *acl-name* 命令通过指定名称的方式进入其视图。

2. 配置 IPv6 高级 ACL

IPv6 高级 ACL 可以使用报文的源 IPv6 地址信息、目的 IPv6 地址信息、IPv6 承载的协议类型、协议的特性（例如 TCP 或 UDP 的源端口、目的端口，ICMP 协议的消息类型、消息码等）等信息来制定匹配规则。

用户可以利用 IPv6 高级 ACL 定义比 IPv6 基本 ACL 更准确、丰富、灵活的规则。

表1-8 配置 IPv6 高级 ACL

操作	命令	说明
进入系统视图	**system-view**	-
创建 IPv6 高级 ACL，并进入 IPv6 高级 ACL 视图	**acl ipv6 number** *acl6-number* [**name** *acl6-name*] [**match-order** { **auto** | **config** }]	必选 缺省情况下，不存在任何 ACL IPv6 高级 ACL 的编号范围 3000～3999
配置 ACL 的描述信息	**description** *text*	可选 缺省情况下，ACL 没有任何描述信息
配置规则编号的步长	**step** *step-value*	可选 缺省情况下，规则编号的步长为 5
创建规则	**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 dest-prefix* | *dest/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** | **source** { *source source-prefix* | *source/source-prefix* **| any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name*] *	必选 缺省情况下，IPv6 高级 ACL 内不存在任何规则 重复执行本命令可以创建多条规则 需要注意的是，当 IPv6 高级 ACL 被 QoS 策略引用对报文进行流分类时： • 不支持配置 **fragment** 参数 • 在规则中配置的 **logging** 和 **counting** 参数不会生效 • 不支持配置操作符 *operator* 取值为 **neq** 当 IPv6 高级 ACL 用于包过滤功能时，不支持配置操作符 *operator* 取值为 **neq**
配置规则的描述信息	**rule** *rule-id* **comment** *text*	可选 缺省情况下，规则没有任何描述信息
使能基于硬件应用的 ACL 规则匹配统计功能	**hardware-count enable**	可选 缺省情况下，基于硬件应用的 ACL 规则匹配统计功能处于关闭状态 当 ACL 被 QoS 策略引用对报文进行流分类时，本功能不会生效

说明

如果在创建 IPv6 高级 ACL 时为其指定了名称，则也可以使用 **acl ipv6 name** *acl6-name* 命令通过指定名称的方式进入其视图。

1.3.4 配置二层 ACL

二层 ACL 根据报文的源 MAC 地址、目的 MAC 地址、802.1p 优先级、二层协议类型等二层信息制定匹配规则，对报文进行相应的分析处理。

表1-9 配置二层 ACL

操作	命令	说明
进入系统视图	**system-view**	-
创建二层 ACL，并进入二层 ACL 视图	**acl number** *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]	必选 缺省情况下，不存在任何 ACL 二层 ACL 的编号范围为 4000～4999
配置 ACL 的描述信息	**description** *text*	可选 缺省情况下，ACL 没有任何描述信息
配置规则编号的步长	**step** *step-value*	可选 缺省情况下，规则编号的步长为 5
创建规则	**rule** [*rule-id*] { **deny** | **permit** } [**cos** *vlan-pri* | **counting** | **dest-mac** *dest-addr dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *sour-addr source-mask* | **time-range** *time-range-name*] *	必选 缺省情况下，二层 ACL 内不存在任何规则 重复执行本命令可以创建多条规则
配置规则的描述信息	**rule** *rule-id* **comment** *text*	可选 缺省情况下，规则没有任何描述信息
使能基于硬件应用的 ACL 规则匹配统计功能	**hardware-count enable**	可选 缺省情况下，基于硬件应用的 ACL 规则匹配统计功能处于关闭状态 当 ACL 被 QoS 策略引用对报文进行流分类时，本功能不会生效

说明

如果在创建二层 ACL 时为其指定了名称，则也可以使用 **acl name** *acl-name* 命令通过指定名称的方式进入其视图。

1.3.5 配置 ACL 规则注释

说明

目前仅支持为 IPv4 ACL 和二层 ACL 配置规则注释。

在一个 ACL 中，用户可以创建多条规则，这些规则可能会用于不同的功能。虽然用户可以通过配置规则的描述信息来标识规则的用途，但是当连续配置的大量规则都用于同一功能时，为每条规则都配置相同描述信息的方式会增加大量配置，且效率低下。

这种情况下，用户可以使用 ACL 规则注释功能，在一段连续规则的开头和结尾处增加注释，便可以在显示 ACL 的规则时，通过注释快速了解一段规则的用途。

需要注意的是，在设备上显示 ACL 规则时，对于不同匹配顺序的 ACL（配置顺序或自动排序），设备输出信息的排列方式不同。在为这两种匹配顺序的 ACL 配置规则注释时，可以分别采用以下方式：

- 对于匹配顺序为“配置顺序”的 ACL，设备在显示规则时将按照规则编号由小到大进行输出。因此，可以通过为注释指定恰当的规则编号，调整其所处的位置，使其准确的显示在一段规则的两端。
- 对于匹配顺序为“自动排序”的 ACL，设备在显示规则时将按照用户配置规则的顺序进行输出。在配置开头注释时，需要将规则编号指定为需要标识的规则段中第一条规则的编号；在配置结尾注释时，需要将规则编号指定为规则段结束后下一条规则的编号，才能使注释信息显示在规则段的两端。

表1-10 配置 ACL 规则注释信息

操作	命令	说明
进入系统视图	**system-view**	-
进入 IPv4 ACL 或二层 ACL 视图	**acl number** *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]	-
配置 ACL 规则注释信息	**rule** [*rule-id*] **remark** *text*	必选 缺省情况下，没有配置 ACL 规则注释信息

说明

配置 ACL 规则注释信息时输入的规则编号主要用于调整注释信息的显示位置，该编号可以与现有规则编号相同，并不影响规则的匹配功能。

1.3.6 复制 ACL

用户可以通过复制一个已存在的 ACL，来生成一个新的同类型 ACL。除了 ACL 的编号和名称不同外，新生成的 ACL（即目的 ACL）的匹配顺序、规则匹配统计功能的使能情况、规则编号的步长、所包含的规则、规则的描述信息以及 ACL 的描述信息等都与源 ACL 的相同。

1. 复制 IPv4 ACL

表1-11 复制 IPv4 ACL

操作	命令	说明
进入系统视图	**system-view**	-
复制生成一个新的同类型 IPv4 ACL	**acl copy** { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }	必选

说明

目的 IPv4 ACL 的类型要与源 IPv4 ACL 的类型相同，且源 IPv4 ACL 必须存在，目的 IPv4 ACL 必须不存在。

2. 复制 IPv6 ACL

表1-12 复制 IPv6 ACL

操作	命令	说明
进入系统视图	**system-view**	-
复制生成一个新的同类型 IPv6 ACL	**acl ipv6 copy** { *source-acl6-number* | **name** *source-acl6-name* } **to** { *dest-acl6-number* | **name** *dest-acl6-name* }	必选

说明

目的 IPv6 ACL 的类型要与源 IPv6 ACL 的类型相同，且源 IPv6 ACL 必须存在，目的 IPv6 ACL 必须不存在。

1.3.7 应用 ACL 进行报文过滤

通过将配置好的不同类型的 ACL 规则应用到指定以太网端口/VLAN 接口的入或出方向上，可以对该端口/VLAN 接口收到或发出的相应类型报文（包括 IPv4 报文和 IPv6 报文）进行过滤。

此外，通过配置报文过滤日志的生成与发送周期，还可以周期性地生成并发送报文过滤的日志信息，包括该周期内被匹配的报文数量以及所使用的 ACL 规则。

说明

- 在 VLAN 接口上应用 ACL 进行报文过滤时，只能对通过该接口进行三层转发的报文进行过滤，而对纯二层转发的报文不进行过滤。
- 系统只支持对应用基本或高级 ACL 进行报文过滤的日志进行记录，且在上述 ACL 中配置规则时须指定 **logging** 参数。
- 对用于报文过滤的 ACL，不支持在规则中配置 **vpn-instance** 参数。
- 报文过滤的日志信息（信息级别为 informational）将被发往信息中心，有关信息中心的详细介绍，请参见“网络管理和监控配置指导”中的“信息中心配置”。

1. 应用 IPv4 ACL 进行报文过滤

表1-13 应用 IPv4 ACL 进行报文过滤

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
进入二层以太网端口视图、三层以太网端口视图或 VLAN 接口视图	**interface** *interface-type interface-number*	-
应用 IPv4 ACL 对 IPv4 报文进行过滤	**packet-filter** { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }	必选 缺省情况下，在以太网端口/VLAN 接口上不对 IPv4 报文进行过滤
退回系统视图	**quit**	-
配置 IPv4 报文过滤日志的生成与发送周期	**acl logging frequence** *frequence*	必选 缺省情况下，IPv4 报文过滤日志的生成与发送周期为 0 分钟，即不记录 IPv4 报文过滤的日志

2. 应用 IPv6 ACL 进行报文过滤

表1-14 应用 IPv6 ACL 进行报文过滤

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图、三层以太网端口视图或 VLAN 接口视图	**interface** *interface-type interface-number*	-
应用 IPv6 ACL 对 IPv6 报文进行过滤	**packet-filter ipv6** { *acl6-number* | **name** *acl6-name* } { **inbound** | **outbound** }	必选 缺省情况下，在以太网端口/VLAN 接口上不对 IPv6 报文进行过滤
退回系统视图	**quit**	-
配置 IPv6 报文过滤日志的生成与发送周期	**acl ipv6 logging frequence** *frequence*	必选 缺省情况下，IPv6 报文过滤日志的生成与发送周期为 0 分钟，即不记录 IPv6 报文过滤的日志

1.4 ACL 显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示 ACL 配置后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 ACL 的统计信息。

表1-15 ACL 显示和维护

配置	命令
显示 IPv4 ACL 的配置和运行情况	**display acl** { *acl-number* | **all** | **name** *acl-name* } [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示 IPv6 ACL 的配置和运行情况	**display acl ipv6** { *acl6-number* | **all** | **name** *acl6-name* } [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

配置	命令
显示 ACL 资源的使用情况	**display acl resource** [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示报文过滤策略的应用情况	**display packet-filter** { { **all** | **interface** *interface-type interface-number* } [**inbound** | **outbound**] | **interface vlan-interface** *vlan-interface-number* [**inbound** | **outbound**] [**slot** *slot-number*] } [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示时间段的配置和状态信息	**display time-range** { *time-range-name* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除 IPv4 ACL 统计信息	**reset acl counter** { *acl-number* | **all** | **name** *acl-name* }
清除 IPv6 ACL 统计信息	**reset acl ipv6 counter** { *acl6-number* | **all** | **name** *acl6-name* }

1.5 ACL 典型配置举例

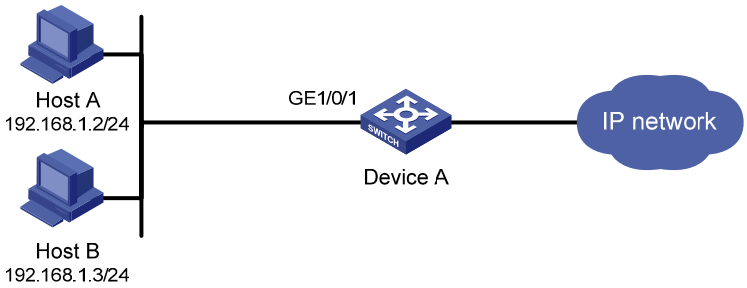
1.5.1 应用 IPv4 ACL 进行报文过滤配置举例

1. 组网需求

要求通过在 Device A 的端口 GigabitEthernet1/0/1 上配置 IPv4 报文过滤功能，实现在每天的 8 点到 18 点期间只允许来自 Host A 的报文通过，并以 10 分钟为周期记录 IPv4 报文过滤的日志信息并输出至控制台。

2. 组网图

图1-1 应用 IPv4 ACL 进行报文过滤配置组网图



3. 配置步骤

创建名为 study 的时间段，其时间范围为每天的 8 点到 18 点。

```
<DeviceA> system-view
[DeviceA] time-range study 8:0 to 18:0 daily
```

创建 IPv4 基本 ACL 2009，并定义如下规则：在名为 study 的时间段内只允许来自 Host A（192.168.1.2）的报文通过、禁止来自其它 IP 地址的报文通过，且在这些规则中对符合条件的报文记录日志信息。

```
[DeviceA] acl number 2009
[DeviceA-acl-basic-2009] rule permit source 192.168.1.2 0 time-range study logging
[DeviceA-acl-basic-2009] rule deny source any time-range study logging
[DeviceA-acl-basic-2009] quit
```

应用 IPv4 基本 ACL 2009 对端口 GigabitEthernet1/0/1 收到的 IPv4 报文进行过滤。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] packet-filter 2009 inbound
```

```
[DeviceA-GigabitEthernet1/0/1] quit
```
配置 IPv4 报文过滤日志的生成与发送周期为 10 分钟。
```
[DeviceA] acl logging frequence 10
```
配置系统信息的输出规则，将级别为 informational 的日志信息输出至控制台。
```
[DeviceA] info-center source default channel 0 log level informational
```

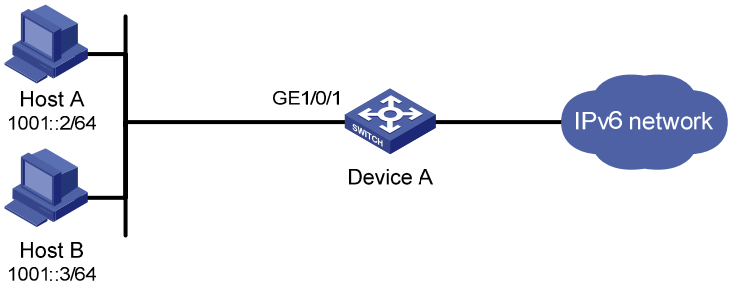
1.5.2 应用 IPv6 ACL 进行报文过滤配置举例

1. 组网需求

要求通过在 Device A 的端口 GigabitEthernet1/0/1 上配置 IPv6 报文过滤功能，实现在每天的 8 点到 18 点期间只允许来自 Host A 的报文通过，并以 10 分钟为周期记录 IPv6 报文过滤的日志信息并输出至控制台。

2. 组网图

图1-2 应用 IPv6 ACL 进行报文过滤配置组网图



3. 配置步骤

创建名为 study 的时间段，其时间范围为每天的 8 点到 18 点。
```
<DeviceA> system-view
[DeviceA] time-range study 8:0 to 18:0 daily
```
创建 IPv6 基本 ACL 2009，并定义如下规则：在名为 study 的时间段内只允许来自 Host A（1001::2）的报文通过、禁止来自其它 IPv6 地址的报文通过，且在这些规则中对符合条件的报文记录日志信息。
```
[DeviceA] acl ipv6 number 2009
[DeviceA-acl6-basic-2009] rule permit source 1001::2 128 time-range study logging
[DeviceA-acl6-basic-2009] rule deny source any time-range study logging
[DeviceA-acl6-basic-2009] quit
```
应用 IPv6 基本 ACL 2009 对端口 GigabitEthernet1/0/1 收到的 IPv6 报文进行过滤。
```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] packet-filter ipv6 2009 inbound
[DeviceA-GigabitEthernet1/0/1] quit
```
配置 IPv6 报文过滤日志的生成与发送周期为 10 分钟。
```
[DeviceA] acl ipv6 logging frequence 10
```
配置系统信息的输出规则，将级别为 informational 的日志信息输出至控制台。
```
[DeviceA] info-center source default channel 0 log level informational
```