

目 录

ACL..... 1

 IPv4 ACL简介..... 1

 IPv4 ACL分类..... 1

 IPv4 ACL命名..... 1

 IPv4 ACL匹配顺序..... 2

 IPv4 ACL步长..... 3

 IPv4 ACL生效时间段..... 3

 IPv4 ACL对分片报文的处理..... 4

 IPv6 ACL简介..... 4

 IPv6 ACL分类..... 4

 IPv6 ACL命名..... 4

 IPv6 ACL匹配顺序..... 5

 IPv6 ACL步长..... 6

 IPv6 ACL生效时间段..... 6

 流模板简介..... 6

ACL

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。

IPv4 ACL 简介

IPv4 ACL 分类

IPv4 ACL根据ACL序号来区分不同的ACL，可以分为四种类型，如 表 1所示。

表1 IPv4 ACL 分类

IPv4 ACL 类型	ACL 序号范围	区分报文的依据
基本 IPv4 ACL	2000～2999	只根据报文的源 IP 地址信息制定匹配规则
高级 IPv4 ACL	3000～3999	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
二层 ACL	4000～4999	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
用户自定义 ACL	5000～5999	可以以报文的报文头、IP 头等为基准，指定从第几个字节开始与掩码进行“与”操作，将从报文提取出来的字符串和用户定义的字符串进行比较，找到匹配的报文

IPv4 ACL 命名

用户在创建 IPv4 ACL 时，可以为 ACL 指定一个名称。每个 IPv4 ACL 最多只能有一个名称。命名的 ACL 使用户可以通过名称唯一地确定一个 IPv4 ACL，并对其进行相应的操作。

在创建 ACL 时，用户可以选择是否配置名称。ACL 创建后，不允许用户修改或者删除 ACL 名称，也不允许为未命名的 ACL 添加名称。

 说明:

IPv4 ACL 的名称对于 IPv4 ACL 全局唯一，但允许与 IPv6 ACL 使用相同的名称。

IPv4 ACL 匹配顺序

一个 ACL 中可以包含多个规则，而每个规则都指定不同的报文匹配选项，这些规则可能存在重复或矛盾的地方，在将一个报文和 ACL 的规则进行匹配的时候，到底采用哪些规则呢？就需要确定规则的匹配顺序。

IPv4 ACL 支持两种匹配顺序：

- 配置顺序：按照用户配置规则的先后顺序进行规则匹配。
- 自动排序：按照“深度优先”的顺序进行规则匹配。

1. 基本 IPv4 ACL 的“深度优先”顺序判断原则如下

- (1) 先看规则中是否带 VPN 实例，带 VPN 实例的规则优先；
- (2) 再比较源 IP 地址范围，源 IP 地址范围小（反掩码中“0”位的数量多）的规则优先；
- (3) 如果源 IP 地址范围相同，则先配置的规则优先。

2. 高级 IPv4 ACL 的“深度优先”顺序判断原则如下

- (1) 先看规则中是否带 VPN 实例，带 VPN 实例的规则优先；
- (2) 再比较协议范围，指定了 IP 协议承载的协议类型的规则优先；
- (3) 如果协议范围相同，则比较源 IP 地址范围，源 IP 地址范围小（反掩码中“0”位的数量多）的规则优先；
- (4) 如果协议范围、源 IP 地址范围相同，则比较目的 IP 地址范围，目的 IP 地址范围小（反掩码中“0”位的数量多）的规则优先；
- (5) 如果协议范围、源 IP 地址范围、目的 IP 地址范围相同，则比较四层端口号（TCP/UDP 端口号）范围，四层端口号范围小的规则优先；
- (6) 如果上述范围都相同，则先配置的规则优先。

3. 二层 ACL 的“深度优先”顺序判断原则如下

- (1) 先比较源 MAC 地址范围，源 MAC 地址范围小（掩码中“1”位的数量多）的规则优先；
- (2) 如果源 MAC 地址范围相同，则比较目的 MAC 地址范围，目的 MAC 地址范围小（掩码中“1”位的数量多）的规则优先；
- (3) 如果源 MAC 地址范围、目的 MAC 地址范围相同，则先配置的规则优先。

 说明:

用户自定义 ACL 的匹配顺序只能为配置顺序。

在报文匹配规则时，会按照匹配顺序去匹配定义的规则，一旦有一条规则被匹配，报文就不再继续匹配其它规则了，设备将对该报文执行第一次匹配的规则指定的动作。

IPv4 ACL 步长

1. 步长的含义

步长的含义是：设备自动为 ACL 规则分配编号的时候，每个相邻规则编号之间的差值。例如，如果将步长设定为 5，规则编号分配是按照 0、5、10、15...这样的规律分配的。缺省情况下，步长为 5。

当步长改变后，ACL 中的规则编号会自动从 0 开始重新排列。例如，原来规则编号为 5、10、15、20，当通过命令把步长改为 2 后，则规则编号变成 0、2、4、6。

当使用命令将步长恢复为缺省值后，设备将立刻按照缺省步长调整 ACL 规则的编号。例如：ACL 3001，步长为 2，下面有 4 个规则，编号为 0、2、4、6。如果此时使用命令将步长恢复为缺省值，则 ACL 规则编号变成 0、5、10、15，步长为 5。

2. 步长的作用

使用步长设定的好处是用户可以方便地在规则之间插入新的规则。例如配置好了 4 个规则，规则编号为：0、5、10、15。此时如果用户希望能在第一条规则之后插入一条规则，则可以使用命令在 0 和 5 之间插入一条编号为 1 的规则。

另外，在定义一条 ACL 规则的时候，用户可以不指定规则编号，这时，系统会从 0 开始，按照步长，自动为规则分配一个大于现有最大编号的最小编号。假设现有规则的最大编号是 28，步长是 5，那么系统分配给新定义的规则的编号将是 30。

IPv4 ACL 生效时间段

时间段用于描述一个特殊的时间范围。用户可能有这样的需求：一些 ACL 规则需要在某个或某些特定时间内生效，而在其他时间段则不利用它们进行报文过滤，即通常所说的按时间段过滤。这时，用户就可以先配置一个或多个时间段，然后在相应的规则下通过时间段名称引用该时间段，这条规则只在该指定的时间段内生效，从而实现基于时间段的 ACL 过滤。

如果规则引用的时间段未配置，则系统给出提示信息，并允许这样的规则创建成功，但是规则不能立即生效，直到用户配置了引用的时间段，并且系统时间在指定时间段范围内 ACL 规则才能生效。

IPv4 ACL 对分片报文的处理

传统的报文过滤并不处理所有 IP 报文分片，而是只对首片（第一片）分片报文进行匹配处理，对后续分片不进行匹配处理。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。

目前，设备提供的对分片报文过滤的功能如下：

- 对所有的分片报文进行三层（IP 层）的匹配过滤。
- 对于包含高级信息的 ACL 规则项（例如包含 TCP/UDP 端口号，ICMP 类型），提供标准匹配和精确匹配两种匹配方式，缺省的匹配方式为标准匹配。

 说明：

标准匹配和精确匹配的含义如下：

- 标准匹配：只匹配三层信息，而三层以外的信息将被忽略。
 - 精确匹配：对 ACL 定义的所有的规则项进行匹配。
-

IPv6 ACL 简介

IPv6 ACL 分类

IPv6 ACL 根据 ACL 序号来区分不同的 ACL，可以分为三种类型，如表 2 所示。

表2 IPv6 ACL 分类

IPv6 ACL 类型	ACL 序号范围	区分报文的依据
基本 IPv6 ACL	2000~2999	只根据源 IPv6 地址信息制定匹配规则
高级 IPv6 ACL	3000~3999	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、协议的特性等三层、四层信息来制定匹配规则
简单 IPv6 ACL	10000~42767	根据报文的源 IPv6 地址信息、目的 IPv6 地址信息、IPv6 地址组合标记、IPv6 承载的协议类型、协议的特性等三层、四层信息来制定匹配规则 简单 IPv6 ACL 在 TCP 标记、分片报文标记上有更丰富的内容

IPv6 ACL 命名

用户在创建 IPv6 ACL 时，可以为 ACL 指定一个名称。每个 IPv6 ACL 最多只能有一个名称。命名的 ACL 使用户可以通过名称唯一地确定一个 IPv6 ACL，并对其进行相应的操作。

在创建 ACL 时，用户可以选择是否配置名称。ACL 创建后，不允许用户修改或者删除 ACL 名称，也不允许为未命名的 ACL 添加名称。

 说明：

- IPv6 ACL 的名称对于 IPv6 ACL 全局唯一，但允许与 IPv4 ACL 使用相同的名称。
 - 简单 IPv6 ACL 不支持命名。
-

IPv6 ACL 匹配顺序

一个 ACL 中可以包含多个规则，而每个规则都指定不同的报文匹配选项，这些规则可能存在重复或矛盾的地方，在将一个报文和 ACL 的规则进行匹配的时候，到底采用哪些规则呢？就需要确定规则的匹配顺序。

IPv6 ACL 支持两种匹配顺序：

- 配置顺序：按照用户配置规则的先后顺序进行规则匹配。
- 自动排序：按照“深度优先”的顺序进行规则匹配。

1. 基本 IPv6 ACL 的“深度优先”顺序判断原则如下

- (1) 先比较源 IPv6 地址范围，源 IPv6 地址范围小（前缀长）的规则优先；
- (2) 如果源 IPv6 地址范围相同，则先配置的规则优先。

2. 高级 IPv6 ACL 的“深度优先”顺序判断原则如下

- (1) 先比较协议范围，指定了 IPv6 协议承载的协议类型的规则优先；
- (2) 如果协议范围相同，则比较源 IPv6 地址范围，源 IPv6 地址范围小（前缀长）的规则优先；
- (3) 如果协议范围、源 IPv6 地址范围相同，则比较目的 IPv6 地址范围，目的 IPv6 地址范围小（前缀长）的规则优先；
- (4) 如果协议范围、源 IPv6 地址范围、目的 IPv6 地址范围相同，则比较四层端口号（TCP/UDP 端口号）范围，四层端口号范围小的规则优先；
- (5) 如果上述范围都相同，则先配置的规则优先。

 说明：

简单 IPv6 ACL 只能定义一条规则，不涉及匹配顺序。

在报文匹配规则时，会按照匹配顺序去匹配定义的规则，一旦有一条规则被匹配，报文就不再继续匹配其它规则了，设备将对该报文执行第一次匹配的规则指定的动作。

IPv6 ACL 步长

关于步长的介绍请参见“IPv4 ACL步长”。

IPv6 ACL 生效时间段

关于生效时间段的介绍请参见“IPv4 ACL生效时间段”。

流模板简介

流模板的主要功能是对硬件下发的 ACL 规则中所能包含的信息进行限制。在接口下发的 ACL 规则中包含的信息必须是该接口下发流模板中定义信息的子集。比如，流模板定义了源 IP 地址、目的 IP 地址、源 TCP 端口、目的 TCP 端口等限制，只有在上述范围内的 ACL 规则可以正确下发到硬件中，用于包过滤、QoS 等功能；否则 ACL 规则将不能下发到硬件中，导致包过滤、QoS 等功能不能引用此 ACL 规则。

设备支持的流模板包括缺省流模板和用户自定义流模板。其中，用户自定义流模板又可分为标准型和扩展型。初始状态下，接口下默认配置缺省流模板。

流模板在全局配置，在接口应用。



注意：

流模板只对基于硬件处理的 ACL 有效，对基于软件处理的 ACL 不生效。
