目 录

第1章 ACL 配置

1.1 ACL 简介

ACL（Access Control List，访问控制列表）主要用来实现流识别功能。网络设备为了过滤数据包，需要配置一系列的匹配规则，以识别需要过滤的报文。在识别出特定的报文之后，才能根据预先设定的策略允许或禁止相应的数据包通过。

ACL 通过一系列的匹配条件对数据包进行分类，这些条件可以是数据包的源地址、目的地址、端口号等。

由 ACL 定义的数据包匹配规则，可以被其它需要对流量进行区分的功能引用，如 QoS 中流分类规则的定义。

根据应用目的，可将 ACL 分为下面几种：

- 基本 ACL：只根据三层源 IP 地址制定规则。
- 高级 ACL：根据数据包的源 IP 地址信息、目的 IP 地址信息、IP 承载的协议类型、协议特性等三、四层信息制定规则。
- 二层 ACL：根据源 MAC 地址、目的 MAC 地址、VLAN 优先级、二层协议类型等二层信息制定规则。
- 用户自定义 ACL：以数据包的头部为基准，指定从第几个字节开始进行“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。

1.1.1 ACL 在交换机上的应用方式

1. ACL 直接下发到硬件中的情况

交换机中ACL可以直接下发到交换机的硬件中用于数据转发过程中报文的过滤和流分类。此时一条 ACL 中多个规则的匹配顺序是由交换机的硬件决定的，用户即使在定义 ACL 时配置了匹配顺序，该匹配顺序也不起作用。

ACL 直接下发到硬件的情况包括：交换机实现 QoS 功能时引用 ACL、通过 ACL 过滤转发数据等。

2. ACL 被上层模块引用的情况

交换机也使用 ACL 来对由软件处理的报文进行过滤和流分类。此时 ACL 规则的匹配顺序有两种：**config**（指定匹配该规则时按用户的配置顺序）和 **auto**（指定匹配该规则时系统自动排序，即按“深度优先”的顺序）。这种情况下用户可以在定义

ACL 的时候指定一条 ACL 中多个规则的匹配顺序。用户一旦指定某一条 ACL 的匹配顺序，就不能再更改该顺序。只有把该列表中所有的规则全部删除后，才能重新指定其匹配顺序。

ACL 被软件引用的情况包括：路由策略引用 ACL、对登录用户进行控制时引用 ACL 等。

1.1.2 ACL 匹配顺序

ACL 可能会包含多个规则，而每个规则都指定不同的报文范围。这样，在匹配报文时就会出现匹配顺序的问题。

ACL 支持两种匹配顺序：

- 配置顺序：根据配置顺序匹配 ACL 规则。
- 自动排序：根据“深度优先”规则匹配 ACL 规则。

“深度优先”顺序的判断原则如下：

(1) 先比较规则的协议范围。IP 协议的范围为 1～255，其他协议的范围就是自己的协议号；协议范围小的优先；

(2) 再比较源 IP 地址范围。源 IP 地址范围小(掩码长)的优先；

(3) 然后比较目的 IP 地址范围。目的 IP 地址范围小(掩码长)的优先；

(4) 最后比较四层端口号（TCP/UDP 端口号）范围。四层端口号范围小的优先；

如果规则 A 与规则 B 按照原有匹配顺序进行配置时，协议范围、源 IP 地址范围、目的 IP 地址范围、四层端口号范围完全相同，并且其它的元素个数相同，将按照加权规则进行排序。加权规则如下：

- 设备为每个元素设定一个固定的权值，最终的匹配顺序由各个元素的权值和元素取值来决定。各个元素自身的权值从大到小排列：DSCP、ToS、ICMP、established、precedence、fragment。
- 设备以一个固定权值依次减去规则各个元素自身的权值，剩余权值越小的规则越优先。
- 如果各个规则中元素个数、元素种类完全相同，则这些元素取值的累加和越小越优先。

1.1.3 基于时间段的 ACL

基于时间段的 ACL 使用户可以区分时间段对报文进行 ACL 控制。

ACL 中的每条规则都可选择一个时间段。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才能生效。如果用户手工删除 ACL 规则引用的时间段，则在 ACL 规则定时器刷新后，该规则将失效。

1.1.4 以太网交换机支持的 ACL

Quidway S3900 系列以太网交换机支持的 ACL 如下：

- 基本 ACL
- 高级 ACL
- 二层 ACL
- 用户自定义 ACL

1.2 配置时间段

对时间段的配置有如下内容：配置周期时间段和绝对时间段。配置周期时间段采用的是每周的周几的形式，配置绝对时间段采用从起始时间到结束时间的形式。

📖 **说明：**

Quidway S3900 系列以太网交换机支持的绝对时间段范围从 1970/1/1 00:00 起至 2100/12/31 24:00 结束。

1.2.1 配置过程

表1-1 配置时间段

配置步骤	命令	说明
进入系统视图	**system-view**	-
创建一个时间段	**time-range** *time-name* { *start-time* **to** *end-time days-of-the-week* [**from** *start-time start-date*] [**to** *end-time end-date*] | **from** *start-time start-date* [**to** *end-time end-date*] | **to** *end-time end-date* }	必选

需要注意的是：

如果一个时间段只定义了周期时间段，则只有系统时钟在该周期时间段内，该时间段才进入激活状态。如果一个时间段下定义了多个周期时间段，则这些周期时间段之间是“或”的关系。

如果一个时间段只定义了绝对时间段，则只有系统时钟在该绝对时间段内，该时间段才进入激活状态。如果一个时间段下定义了多个绝对时间段，则这些绝对时间段之间是“或”的关系。

如果一个时间段同时定义了绝对时间段和周期时间段，则只有同时满足绝对时间段和周期时间段的定义时，该时间段才进入激活状态。例如，一个时间段定义了绝对时间段：从 2004 年 1 月 1 日 0 点 0 分到 2004 年 12 月 31 日 23 点 59 分，同时定义了周期时间段：每周三的 12：00 到 14：00。该时间段只有在 2004 年内每周三的 12：00 到 14：00 才进入激活状态。

配置绝对时间段时，如果不配置开始日期，时间段就是从系统支持的最早时间起到配置的结束日期为止。如果不配置结束日期，时间段就是从配置的开始日期起到 2100/12/31 23:59 为止。

1.2.2 配置举例

配置周期时间段，取值为周一到周五每天 8:00 到 18:00。

```
<Quidway> system-view
[Quidway] time-range test 8:00 to 18:00 working-day
[Quidway] display time-range test
Current time is 13:27:32 4/16/2005 Saturday

Time-range : test ( Inactive )
 08:00 to 18:00 working-day
```

配置绝对时间段，取值为 2000 年 1 月 28 日 15:00 起至 2004 年 1 月 28 日 15:00 结束。

```
<Quidway> system-view
[Quidway] time-range test from 15:00 1/28/2000 to 15:00 1/28/2004
[Quidway] display time-range test
Current time is 13:30:32 4/16/2005 Saturday

Time-range : test ( Inactive )
 From 15:00 Jan/28/2000 to 15:00 Jan/28/2004
```

1.3 定义基本 ACL

基本 ACL 只根据三层源 IP 制定规则，对数据包进行相应的分析处理。

基本 ACL 的序号取值范围为 2000～2999。

1.3.1 配置准备

如果要配置带有时间段参数的规则，则需要定义相应的时间段。定义时间段的配置请参见1.2 配置时间段。

确定了规则中源 IP 地址信息的取值。

1.3.2 配置过程

表1-2 定义基本 ACL 规则

配置步骤	命令	说明
进入系统视图	**system-view**	-
创建或进入基本 ACL 视图	**acl number** *acl-number* [**match-order** { **config** | **auto** }]	缺省情况下匹配顺序为 **config**
定义 ACL 规则	**rule** [*rule-id*] { **permit** | **deny** } [**fragment** | **source** { *sour-addr sour-wildcard* | **any** } | **time-range** *time-name*]*	必选
定义 ACL 的描述信息	**description** *text*	可选

对于在定义 ACL 规则时指定编号的情况：

- 当匹配顺序为 **config** 时，如果指定编号对应的规则已经存在，系统将编辑该规则，没有编辑的部分仍旧保持原来的状态；当匹配顺序为 **auto** 时，用户不能编辑任何一个已经存在的规则，否则系统会提示错误信息。
- 如果指定编号对应的规则不存在，用户将创建并定义一个新的规则。
- 编辑后或新创建的规则不能和已经存在的规则内容完全相同，否则会导致编辑或创建不成功，系统会提示该规则已经存在。

在定义 ACL 规则时如果不指定编号，用户将创建并定义一个新规则，设备将自动为这个规则分配一个编号。

1.3.3 配置举例

配置一个 ACL 2000，禁止源地址为 1.1.1.1 的报文通过。

```
<Quidway> system-view
[Quidway] acl number 2000
[Quidway-acl-basic-2000] rule deny source 1.1.1.1 0
[Quidway-acl-basic-2000] display acl 2000
Basic ACL  2000, 1 rule
Acl's step is 1
rule 0 deny source 1.1.1.1 0
```

1.4 定义高级 ACL

高级 ACL 可以使用数据包的源地址信息、目的地址信息、IP 承载的协议类型、针对协议的特性，例如 TCP 或 UDP 的源端口、目的端口，ICMP 协议的类型、code 等内容定义规则。

高级 ACL 序号取值范围 3000～3999（ACL 3998 与 3999 是系统为集群管理预留的编号，用户无法配置）。

高级 ACL 支持对三种报文优先级的分析处理：ToS（Type Of Service，服务类型）优先级、IP 优先级和 DSCP（Differentiated Services Codepoint Priority，差分服务编码点优先级）。

用户可以利用高级 ACL 定义比基本 ACL 更准确、更丰富、更灵活的规则。

1.4.1 配置准备

如果要配置带有时间段参数的规则，则需要定义相应的时间段。定义时间段的配置请参见1.2 配置时间段。

确定了规则中源 IP 地址信息、目的 IP 信息、IP 承载的协议类型、针对协议的特性等参数的取值。

1.4.2 配置过程

表1-3 定义高级 ACL 规则

配置步骤	命令	说明
进入系统视图	**system-view**	-
创建或进入高级 ACL 视图	**acl number** *acl-number* [**match-order** { **config** | **auto** }]	缺省情况下匹配顺序为 **config**
定义 ACL 规则	**rule** [*rule-id*] { **permit** | **deny** } *rule-string*	必选
定义 ACL 规则的注释字符串	**rule** *rule-id* **comment** *text*	可选
定义 ACL 的描述信息	**description** *text*	可选

rule-string：ACL 规则信息，可以由表 1-4中的参数组合而成，具体参数说明如表 1-4所示。ACL 规则信息中必须首先配置 *protocol* 参数，然后才能配置其他参数。

表1-4 ACL 规则信息

参数	类别	作用	说明
protocol	协议类型	IP 承载的协议类型	用数字表示时取值范围为 1～255 用名字表示时，可以选取 GRE、ICMP、IGMP、IP、IPinIP、OSPF、TCP、UDP
source { *sour-addr sour-wildcard* | **any** }	源地址信息	指定 ACL 规则的源地址信息	*sour-addr sour-wildcard* 用来确定数据包的源地址，点分十进制表示；*sour-wildcard* 可以为 0，表示主机地址 **any** 代表任意源地址

参数	类别	作用	说明
destination { *dest-addr dest-wildcard* | **any** }	目的地址信息	指定 ACL 规则的目的地址信息	*dest-addr dest-wildcard* 用来确定数据包的目的地址，点分十进制表示；*dest-wildcard* 可以为 0，表示主机地址 **any** 代表任意目的地址
precedence *precedence*	报文优先级	IP 优先级	取值范围 0～7
tos *tos*	报文优先级	ToS 优先级	取值范围 0～15
dscp *dscp*	报文优先级	DSCP 优先级	取值范围 0～63
fragment	分片信息	定义规则仅对非首片分片报文有效	-
time-range *time-name*	时间段信息	指定规则生效的时间段	-

如果选择 **dscp** 关键字，除了直接输入数值 0～63 外，用户也可输入如表 1-5所示的关键字。

表1-5 DSCP 值说明

关键字	DSCP 值（十进制）	DSCP 值（二进制）
ef	46	101110
af11	10	001010
af12	12	001100
af13	14	001110
af21	18	010010
af22	20	010100
af23	22	010110
af31	26	011010
af32	28	011100
af33	30	011110
af41	34	100010
af42	36	100100
af43	38	100110
cs1	8	001000
cs2	16	010000
cs3	24	011000

关键字	DSCP 值（十进制）	DSCP 值（二进制）
cs4	32	100000
cs5	40	101000
cs6	48	110000
cs7	56	111000
be (default)	0	000000

如果选择 **precedence** 关键字，除了直接输入数值 0～7 外，用户也可输入如表 1-6 所示的关键字。

表1-6 IP precedence 值说明

关键字	IP Precedence（十进制）	IP Precedence（二进制）
routine	0	000
priority	1	001
immediate	2	010
flash	3	011
flash-override	4	100
critical	5	101
internet	6	110
network	7	111

如果选择 **tos** 关键字，除了直接输入数值 0～15 外，用户也可输入如表 1-7所示的关键字。

表1-7 ToS 值说明

关键字	ToS（十进制）	ToS（二进制）
normal	0	0000
min-monetary-cost	1	0001
max-reliability	2	0010
max-throughput	4	0100
min-delay	8	1000

当协议类型选择为 TCP 或者 UDP 时，用户还可以定义如下信息。

表1-8 TCP/UDP 特有的 ACL 规则信息

参数	类别	作用	说明
source-port *operator port1* [*port2*]	源端口	定义 UDP/TCP 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）；只有操作符 range 需要两个端口号做操作数，其他的只需要一个端口号做操作数 *port1*、*port2*：TCP 或 UDP 的端口号，用名字或数字表示，数字的取值范围为 0～65535
destination-port *operator port1* [*port2*]	目的端口	定义 UDP/TCP 报文的目的端口信息	
established	TCP 连接建立标识	表示此条规则仅对 TCP 建立连接的第一个 SYN 报文有效	TCP 协议特有的参数

当 TCP 或 UDP 的端口号用名字表示时，用户还可以定义如下信息。

表1-9 TCP 或 UDP 端口取值信息

协议类型	取值信息
TCP	**CHARgen**（19）、**bgp**（179）、**cmd**（514）、**daytime**（13）、**discard**（9）、**domain**（53）、**echo**（7）、**exec**（512）、**finger**（79）、**ftp**（21）、**ftp-data**（20）、**gopher**（70）、**hostname**（101）、**irc**（194）、**klogin**（543）、**kshell**（544）、**login**（513）、**lpd**（515）、**nntp**（119）、**pop2**（109）、**pop3**（110）、**smtp**（25）、**sunrpc**（111）、**tacacs**（49）、**talk**（517）、**telnet**（23）、**time**（37）、**uucp**（540）、**whois**（43）、**www**（80）
UDP	**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**（139）、**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）

📖 **说明：**

Quidway S3900 系列以太网交换机在端口上应用高级 ACL 时，只支持配置 *operator* 取值为 eq 的情况。

当协议类型选择为 ICMP 时，用户还可以定义如下信息。

表1-10 ICMP 特有的 ACL 规则信息

参数	类别	作用	说明
icmp-type *icmp-type* *icmp-code*	ICMP 报文的类型和消息码信息	指定规则中 ICMP 报文的类型和消息码信息	*icmp-type*：ICMP 消息类型，取值为 0～255 *icmp-code*：ICMP 的消息码，取值为 0～255

当协议类型选择为 ICMP 时，用户也可以直接在 **icmp-type** 参数后输入 ICMP 的消息名称。在几种常见的 ICMP 消息如表 1-11所示。

表1-11 ICMP 消息

名称	ICMP TYPE	ICMP CODE
echo	Type=8	Code=0
echo-reply	Type=0	Code=0
fragmentneed-DFset	Type=3	Code=4
host-redirect	Type=5	Code=1
host-tos-redirect	Type=5	Code=3
host-unreachable	Type=3	Code=1
information-reply	Type=16	Code=0
information-request	Type=15	Code=0
net-redirect	Type=5	Code=0
net-tos-redirect	Type=5	Code=2
net-unreachable	Type=3	Code=0
parameter-problem	Type=12	Code=0
port-unreachable	Type=3	Code=3
protocol-unreachable	Type=3	Code=2
reassembly-timeout	Type=11	Code=1
source-quench	Type=4	Code=0
source-route-failed	Type=3	Code=5
timestamp-reply	Type=14	Code=0
timestamp-request	Type=13	Code=0
ttl-exceeded	Type=11	Code=0

对于在定义 ACL 规则时指定编号的情况：

- 当匹配顺序为 **config** 时，如果指定编号对应的规则已经存在，系统将编辑该规则，没有编辑的部分仍旧保持原来的状态；当匹配顺序为 **auto** 时，用户不能编辑任何一个已经存在的规则，否则系统会提示错误信息。
- 如果指定编号对应的规则不存在，用户将创建并定义一个新的规则。
- 编辑后或新创建的规则不能和已经存在的规则内容完全相同，否则会导致编辑或创建不成功，系统会提示该规则已经存在。

在定义 ACL 规则时如果不指定编号，用户将创建并定义一个新规则，设备将自动为这个规则分配一个编号。

1.4.3 配置举例

配置 ACL 3000，允许从 129.9.0.0 网段的主机向 202.38.160.0 网段的主机发送的端口号为 80 的 TCP 报文通过。

```
<Quidway> system-view
[Quidway] acl number 3000
[Quidway-acl-adv-3000] rule permit tcp source 129.9.0.0 0.0.255.255
destination 202.38.160.0 0.0.0.255 destination-port eq 80
[Quidway-acl-adv-3000] display acl 3000
Advanced ACL 3000, 1 rule
Acl's step is 1
 rule 0 permit tcp source 129.9.0.0 0.0.255.255 destination 202.38.160.0
0.0.0.255 destination-port eq www
```

1.5 定义二层 ACL

二层 ACL 根据源 MAC 地址、目的 MAC 地址、VLAN 优先级、二层协议类型等二层信息制定规则，对数据进行相应处理。

二层 ACL 的序号取值范围为 4000～4999。

1.5.1 配置准备

如果要配置带有时间段参数的规则，则需要定义相应的时间段。定义时间段的配置请参见1.2 配置时间段。

确定了规则中源 MAC 地址、目的 MAC 地址、VLAN 优先级、二层协议类型等参数的取值。

1.5.2 配置过程

表1-12 定义二层 ACL 规则

配置步骤	命令	说明
进入系统视图	**system-view**	-
创建或进入二层 ACL 视图	**acl number** *acl-number*	必选
定义 ACL 规则	**rule** [*rule-id*] { **permit** | **deny** } *rule-string*	必选
定义 ACL 规则的注释字符串	**rule** *rule-id* **comment** *text*	可选
定义 ACL 的描述信息	**description** *text*	可选

rule-string：ACL 规则信息，可以由表 1-13中的参数组合而成，具体参数说明如表1-13所示。

表1-13 ACL 规则信息

参数	类别	作用	说明
format-type	链路层封装类型	定义规则中的链路层封装类型	*format-type*：取值可以为802.3/802.2、802.3、ether_ii、snap
lsap *lsap-code lsap-wildcard*	lsap 字段	定义规则中的lsap 字段	*lsap-code*：数据帧的封装格式，16 比特的十六进制数 *lsap-wildcard*：Lsap 值的掩码，16 比特的十六进制数，用于指定屏蔽位
source { *source-addr source-mask* | *vlan-id* }*	源 MAC 信息	定义规则的源MAC 地址范围	*source-addr*：源 MAC 地址，格式为 H-H-H *source-mask*：源 MAC 地址的掩码，格式为 H-H-H *vlan-id*：源 VLAN ID，取值范围 1～4094
dest *dest-addr dest-mask*	目的 MAC 信息	定义规则的目的 MAC 地址范围	*dest-addr*：目的 MAC 地址，格式为 H-H-H *dest-mask*：目的 MAC 地址的掩码，格式为 H-H-H
cos *vlan-pri*	优先级	定义规则的802.1p 优先级	*vlan-pri*：取值范围为 0～7
time-range *time-name*	时间段信息	指定规则生效的时间段	*time-name*：指定规则生效的时间段名称，字符串格式，长度为 1～32

参数	类别	作用	说明
type *protocol-type protocol-mask*	以太网帧的协议类型	定义以太网帧的协议类型	*protocol-type*：协议类型 *protocol-mask*：协议类型掩码

📖 **说明：**

- Quidway S3900 系列以太网交换机在端口上应用二层 ACL 时，不支持配置 *format-type* 参数。
- 如果用户在规则中配置了 **lsap** 参数，此规则可以在端口上应用，但不会生效。

如果选择 **cos** 关键字，除了直接输入数值 0～7 外，用户也可输入如表 1-14所示的关键字。

表1-14 CoS 值说明

关键字	CoS（十进制）	CoS（二进制）
best-effort	0	000
background	1	001
spare	2	010
excellent-effort	3	011
controlled-load	4	100
video	5	101
voice	6	110
network-management	7	111

对于在定义 ACL 规则时指定编号的情况：

- 如果指定编号对应的规则已经存在，用户将编辑该规则，规则中编辑后的部分将覆盖原来的内容，未被编辑的部分保持不变；
- 如果指定编号对应的规则不存在，用户将创建并定义一个新的规则。
- 编辑后或新创建的规则不能和已经存在的规则内容完全相同，否则会导致编辑或创建不成功，系统会提示该规则已经存在。

在定义 ACL 规则时如果不指定编号，用户将创建并定义一个新规则，设备将自动为这个规则分配一个编号。

1.5.3 配置举例

配置 ACL 4000，禁止从 MAC 地址 000d-88f5-97ed 发送到 MAC 地址 011-4301-991e 且 802.1p 优先级为 3 的报文通过。

```
<Quidway> system-view
[Quidway] acl number 4000
[Quidway-acl-ethernetframe-4000] rule deny cos 3 source 000d-88f5-97ed
ffff-ffff-ffff dest 0011-4301-991e ffff-ffff-ffff
[Quidway-acl-ethernetframe-4000] display acl 4000
Ethernet frame ACL  4000, 1 rule
Acl's step is 1
 rule 0 deny cos excellent-effort source 000d-88f5-97ed ffff-ffff-ffff dest
0011-4301-991e ffff-ffff-ffff
```

1.6 定义用户自定义 ACL

用户自定义 ACL 以数据包的头部为基准，指定从第几个字节开始进行“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，然后进行相应的处理。

用户自定义 ACL 的序号取值范围为 5000～5999。

1.6.1 配置准备

如果要配置带有时间段参数的规则，则需要定义相应的时间段。定义时间段的配置请参见1.2 配置时间段。

1.6.2 配置过程

表1-15 定义用户自定义 ACL 规则

配置步骤	命令	说明
进入系统视图	**system-view**	-
创建或进入用户自定义 ACL 视图	**acl number** *acl-number*	必选
定义 ACL 规则	**rule** [*rule-id*] { **permit** | **deny** } [*rule-string rule-mask offset*] &<1-8> [**time-range** *name*]	必选
定义 ACL 的描述信息	**description** *text*	可选
定义 ACL 规则的注释字符串	**rule** *rule-id* **comment** *text*	可选

说明：

用户在设置偏移量 *offset* 的数值时一定要考虑如下情况:

- 交换机内部处理的报文都带有 VLAN tag，1 层 VLAN tag 占 4 个字节。
- 如果没有使能 VLAN VPN 功能，交换机内部处理的报文都带有 1 层 VLAN tag。
- 如果某一端口上使能了 VLAN VPN 功能，交换机会给所有端口接收的报文再打 1 层 VLAN tag，无论报文原来是否带有 VLAN tag，报文都将具有 2 层 VLAN tag。

对于在定义 ACL 规则时指定编号的情况：

- 如果指定编号对应的规则已经存在，用户将编辑该规则，规则中编辑后的部分将覆盖原来的内容，未被编辑的部分保持不变；
- 如果指定编号对应的规则不存在，用户将创建并定义一个新的规则。
- 编辑后或新创建的规则不能和已经存在的规则内容完全相同，否则会导致编辑或创建不成功，系统会提示该规则已经存在。

在定义 ACL 规则时如果不指定编号，用户将创建并定义一个新规则，设备将自动为这个规则分配一个编号。

1.6.3 配置举例

配置 ACL 5001，禁止所有的 TCP 报文通过（假设端口上没有启动 VLAN VPN 功能）。

```
<Quidway> system-view
[Quidway] time-range t1 18:00 to 23:00 sat
[Quidway] acl number 5001
[Quidway-acl-user-5001] rule 25 deny 06 ff 27 time-range t1
[Quidway-acl-user-5001] display acl 5001
User defined ACL  5001, 1 rules
Acl's step is 1
rule 25 deny 06 ff 27 time-range t1 (Inactive)
```

1.7 在端口上应用 ACL

在端口上应用ACL可以实现报文过滤的功能，用户可在每个端口上对报文进行过滤。

1.7.1 配置准备

在端口上应用 ACL 之前需要首先定义 ACL。定义 ACL 的配置请参见1.3 定义基本 ACL，1.4 定义高级 ACL，1.5 定义二层 ACL，1.6 定义用户自定义 ACL。

1.7.2 配置过程

表1-16 在端口上应用 ACL

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入以太网端口视图	**interface** *interface-type interface-number*	-
在端口上应用 ACL	**packet-filter** { **inbound** | **outbound** } *acl-rule*	必选

用户在端口上应用的 ACL 可以是多种 ACL 的组合。组合方式说明如下。

表1-17 组合应用 ACL 的方式

组合方式	acl-rule 的形式
单独应用一个 IP 型 ACL 中所有规则	**ip-group** *acl-number*
单独应用一个 IP 型 ACL 中一条规则	**ip-group** *acl-number* **rule** *rule-id*
单独应用一个 Link 型 ACL 中所有规则	**link-group** *acl-number*
单独应用一个 Link 型 ACL 中一条规则	**link-group** *acl-number* **rule** *rule-id*
单独应用一个用户自定义 ACL 中所有规则	**user-group** *acl-number*
单独应用一个用户自定义 ACL 中一条规则	**user-group** *acl-number* **rule** *rule-id*
同时应用 IP 型 ACL 中一条规则和一个 Link 型 ACL 的一条规则	**ip-group** *acl-number* **rule** *rule-id* **link-group** *acl-number* **rule** *rule-id*

1.7.3 配置举例

在 GigabitEthernet 1/1/1 的入方向上应用 ACL 2100 进行包过滤。

```
<Quidway> system-view
[Quidway] interface gigabitethernet 1/1/1
[Quidway-GigabitEthernet1/1/1] packet-filter inbound ip-group 2100
```

1.8 ACL 的显示

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。

表1-18 ACL 的显示

操作	命令	说明
显示配置的 ACL 规则	**display acl** { **all** | *acl-number* }	可选 **display** 命令可以在任意视图下执行
显示时间段	**display time-range** { **all** | *time-name* }	
显示包过滤的应用信息	**display packet-filter** { **interface** *interface-type interface-number* | **unitid** *unit-id* }	

1.9 ACL 典型配置案例

1.9.1 基本 ACL 配置案例

1. 组网需求

通过基本 ACL，实现在每天 8:00～18:00 时间段内对源 IP 为 10.1.1.1 主机发出报文的过滤（该主机从交换机的 GigabitEthernet1/1/1 接入）。

2. 组网图

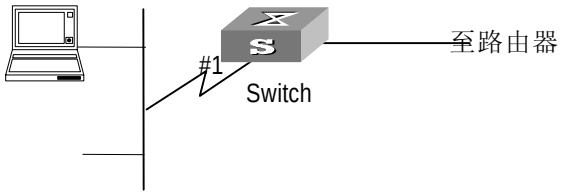

图1-1 访问控制典型配置举例

3. 配置步骤

📖 说明：

以下的配置，只列出了与 ACL 配置相关的命令。

(1) 定义时间段

定义 8:00 至 18:00 的周期时间段。

```
<Quidway> system-view
[Quidway] time-range test 8:00 to 18:00 daily
```

(2) 定义源 IP 为 10.1.1.1 的 ACL

进入 ACL2000 视图。

```
[Quidway] acl number 2000
```

定义源 IP 为 10.1.1.1 的访问规则。

```
[Quidway-acl-basic-2000] rule 1 deny source 10.1.1.1 0 time-range test
[Quidway-acl-basic-2000] quit
```

(3)　在端口上应用 ACL

在端口上应用 ACL 2000。

```
[Quidway] interface gigabitethernet1/1/1
[Quidway-GigabitEthernet1/1/1] packet-filter inbound ip-group 2000
```

1.9.2 高级 ACL 配置案例

1. 组网需求

公司企业网通过 Switch 的端口实现各部门之间的互连。研发部门由 GigabitEthernet1/1/1 接入交换机，工资查询服务器的地址为 192.168.1.2。要求正确配置 ACL，禁止研发部门在工作日 8:00 至 18:00 访问工资服务器。

2. 组网图

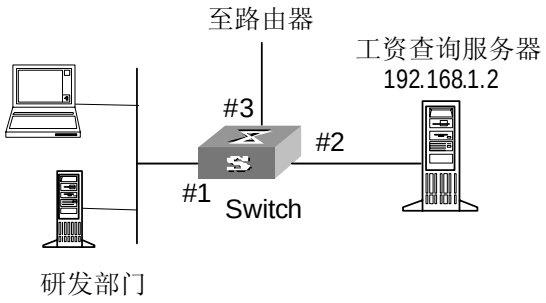

图1-2 访问控制典型配置举例

3. 配置步骤

📖 **说明：**

以下的配置，只列出了与 ACL 配置相关的命令。

---

(1)　定义时间段

定义 8:00 至 18:00 的周期时间段。

```
<Quidway> system-view
[Quidway] time-range test 8:00 to 18:00 working-day
```

(2)　定义到工资服务器的 ACL

进入 ACL3000 视图。

```
[Quidway] acl number 3000
```

定义其它部门到工资服务器的访问规则。

```
[Quidway-acl-adv-3000] rule 1 deny ip destination 192.168.1.2 0 time-range
test
[Quidway-acl-adv-3000] quit
```

(3)　在端口上应用 ACL

在端口上应用 ACL 3000。

```
[Quidway] interface gigabitethernet1/1/1
[Quidway-GigabitEthernet1/1/1] packet-filter inbound ip-group 3000
```

1.9.3 二层 ACL 配置案例

1. 组网需求

通过二层 ACL，实现在每天 8:00～18:00 时间段内对源 MAC 为 00e0-fc01-0101 目的 MAC 为 00e0-fc01-0303 报文的过滤。该二层 ACL 在 GigabitEthernet1/1/1 端口上应用。

2. 组网图

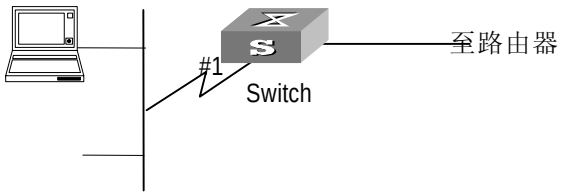

图1-3 访问控制典型配置举例

3. 配置步骤

> 说明：
> 以下的配置，只列出了与 ACL 配置相关的命令。

(1)　定义时间段

定义 8:00 至 18:00 的周期时间段。

```
<Quidway> system-view
[Quidway] time-range test 8:00 to 18:00 daily
```

(2)　定义源 MAC 为 00e0-fc01-0101 目的 MAC 为 00e0-fc01-0303 的 ACL 规则

进入 ACL4000 视图。

```
[Quidway] acl number 4000
```

定义源 MAC 为 00e0-fc01-0101 目的 MAC 为 00e0-fc01-0303 的流分类规则。

```
[Quidway-acl-ethernetframe-4000] rule 1 deny source 00e0-fc01-0101
ffff-ffff-ffff dest 00e0-fc01-0303 ffff-ffff-ffff time-range test
[Quidway-acl-ethernetframe-4000] quit
```

(3) 在端口上应用 ACL

在 GigabitEthernet 1/1/1 端口上应用 ACL。

```
[Quidway] interface GigabitEthernet1/1/1
[Quidway-GigabitEthernet1/1/1] packet-filter inbound link-group 4000
```

1.9.4 用户自定义 ACL 配置案例

1. 组网需求

通过用户自定义 ACL，实现在每天 8:00～18:00 时间段内禁止所有的 TCP 报文通过。该用户自定义 ACL 在 Ethernet1/0/1 端口上应用。

2. 组网图

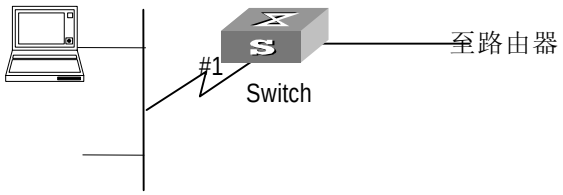

图1-4 访问控制典型配置举例

3. 配置步骤

📖 **说明：**

以下的配置，只列出了与 ACL 配置相关的命令。

---

(1) 定义时间段

定义 8:00 至 18:00 的周期时间段。

```
[Quidway] time-range aaa 8:00 to 18:00 daily
```

(2) 定义 TCP 报文的 ACL

进入 ACL5000 视图。

```
[Quidway] acl number 5000
```

定义 TCP 报文的流分类规则（假设端口上没有启动 VLAN VPN 功能）。

```
[Quidway-acl-user-5000] rule 1 deny 06 ff 27 time-range aaa
```

(3) 在端口上应用 ACL

在 Ethernet 1/0/1 端口上应用 ACL 5000。

```
[Quidway] interface Ethernet1/0/1
[Quidway-Ethernet1/0/1] packet-filter inbound user-group 5000
```