

# 知 通过用户自定义ACL实现过滤ARP报文

ACL 李莹 2023-05-31 发表

组网及说明

不涉及

## 配置步骤

匹配IP报文TTL字段，需要通过用户自定义ACL实现，自定义ACL的序号取值范围为5000~5999。规则配置的命令格式如下：

```
rule [ rule-id ] { permit | deny } [ [ l2 | l4 ] { rule-string rule-mask offset } &<1-8> ] [ time-range time-name ]
```

其中，

l2：从二层帧头开始偏移。

l4：从四层报文头开始偏移。

rule-string：用户自定义的规则字符串，必须是16进制数组成，字符长度必须是偶数。

rule-mask：规则字符串的掩码，用于和报文作“与”操作，必须是16进制数组成，字符长度必须是偶数。

。

offset：偏移量，指定从第几个字节开始进行“与”操作。

&<1-8>：表示一次最多可以定义8个这样的规则。

使用如下rule可以过滤掉arp请求的，这里没有匹配arp的0806，匹配了这个arp报文里面的target ip，也就是目的ip，这种方法能过滤掉arp报文（因为偏移量是固定的，所以不用担心过滤掉其他报文）

```
acl number 5000
```

```
rule 0 deny l2 c0a800fe ffffffff 38 （这里38是因为测试场景没有vlan tag，减去了4 byte，如果有vlan tag就是42）
```

表示从二层以太网帧偏移38个字节，即TTL字段。这里的TTL为默认255

如果是上了cpu的，arp就过滤不了了

Packet capture details for an ARP request:

- Frame 4: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
- Ethernet II, Src: IEF-VRRP-VRID\_01 (00:00:00:00:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- 802.1Q virtual LAN, Prio: 0, DEI: 0, ID: 10
- Address Resolution Protocol (ARP Announcement)
- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: request (1)
- [is gratuitous: True]
- [is announcement: True]
- Sender MAC address: IEF-VRRP-VRID\_01 (00:00:00:00:00:00)
- Sender IP address: 192.168.0.254
- Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
- Target IP address: 192.168.0.254

```
[HundredGigE1/0/0/3]dis thi
```

```
#
```

```
interface HundredGigE1/0/0/3
```

```
port link-mode bridge
```

```
port access vlan 200
```

```
packet-filter user-defined 5000 inbound
```

```
#
```

这个设备去ping远端的124.1.1.1，中间的交换机设备是二层透传，可以看到交换机下发包过滤前是可以通的，下发包过滤后，删除设备上的arp后就无法再学习到arp

```
[2134-S6525XE-HI]ping 124.1.1.1
```

```
Ping 124.1.1.1 (124.1.1.1): 56 data bytes, press CTRL+C to break
```

```
56 bytes from 124.1.1.1: icmp_seq=0 ttl=255 time=1.465 ms
```

```
56 bytes from 124.1.1.1: icmp_seq=1 ttl=255 time=1.259 ms
```

```
56 bytes from 124.1.1.1: icmp_seq=2 ttl=255 time=1.293 ms
```

```
56 bytes from 124.1.1.1: icmp_seq=3 ttl=255 time=1.253 ms
```

```
56 bytes from 124.1.1.1: icmp_seq=4 ttl=255 time=1.195 ms
```

```
--- Ping statistics for 124.1.1.1 ---
```

```
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
```

```
round-trip min/avg/max/std-dev = 1.195/1.293/1.465/0.092 ms
```

```
[2134-SW1]undo arp 124.1.1.1 （这里一定要删除已有的arp表项，不然arp没老化，还是能ping通，因为icmp报文在该场景是过滤不掉的，只能过滤arp）
```

[2134-SW]ping 124.1.1.1

Ping 124.1.1.1 (124.1.1.1): 56 data bytes, press CTRL+C to break

Request time out

#### 配置关键点

- 1、偏移字节数需要根据实际报文来决定，报文携带有VLAN tag，则需要加4个字节，即偏移量为42。
- 2、TTL默认为255，根据实际报文修改

