# IE4300-28P 只让固定mac地址的终端访问网络失败

IP Source Guar | packet-filter | 许鹏鹏 2020-03-16 发表

## 组网及说明

无

## 问题描述

现场想要实现接口下只让固定mac地址的终端访问网络，配置了静态ipv4表项绑定以及配置静态mac地址表，接口下最大mac地址数为0，达到最大mac地址学习数后不转发源MAC地址不在MAC地址表里的数据帧两种方式都无法实现现场需求。

## 过程分析

现场使用了两种方案发现都无法达到这个需求，下面我们来分析下这两种方案

方案一：将接口下mac地址最大学习设置为0

```
interface GigabitEthernet1/0/5
 port access vlan 101
 packet-filter 3300 inbound
 mac-address max-mac-count 0
 mac-address max-mac-count disable-forwarding
 mac-address static 48ea-63db-abcd vlan 101
#
return
[LF-GYMJ-SX1-SW-GigabitEthernet1/0/5]ping -c 1000 10.145.225.166
  PING 10.145.225.166: 56  data bytes, press CTRL_C to break
    Reply from 10.145.225.166: bytes=56 Sequence=1 ttl=64 time=1 ms
    Reply from 10.145.225.166: bytes=56 Sequence=2 ttl=64 time=1 ms
    Reply from 10.145.225.166: bytes=56 Sequence=3 ttl=64 time=2 ms
    Reply from 10.145.225.166: bytes=56 Sequence=4 ttl=64 time=2 ms
```

---

方案二：配置ip source guard将ip和mac绑定

```
#
interface GigabitEthernet1/0/5
 port access vlan 101
 packet-filter 3300 inbound
 ip source binding ip-address 192.168.1.1 mac-address 48ea-63db-abcd
 ip verify source ip-address mac-address
#
return
[LF-GYMJ-SX1-SW-GigabitEthernet1/0/5]ping 10.145.225.166
  PING 10.145.225.166: 56  data bytes, press CTRL_C to break
    Reply from 10.145.225.166: bytes=56 Sequence=1 ttl=64 time=2 ms
    Reply from 10.145.225.166: bytes=56 Sequence=2 ttl=64 time=2 ms
    Reply from 10.145.225.166: bytes=56 Sequence=3 ttl=64 time=2 ms
    Reply from 10.145.225.166: bytes=56 Sequence=4 ttl=64 time=2 ms
Reply from 10.145.225.166: bytes=56 Sequence=5 ttl=64 time=2 ms
```

测试终端连接在G1/0/5口下，远程上去将mac地址表老化时间设置为10s，清空arp表，将接口shutdown后undoshutdown，等待接口收敛完成后ping测试发现接口又马上学习到了arp表和mac地址表，让现场用和该终端同网段的终端ping测试也是可以通的

方案1的问题 ： mac-address max-mac-count 0 只能限制 学习到的MAC, arp添加的MAC 不受限制；

方案2的问题： 接口下还配置了包过滤，包过滤的配置如下：

```
acl number 3300
 rule 10 deny tcp destination-port eq 135
 rule 20 deny tcp destination-port eq 136
 rule 30 deny tcp destination-port eq 137
 rule 40 deny tcp destination-port eq 138
 rule 50 deny tcp destination-port eq 139
 rule 60 deny tcp destination-port eq 445
 rule 70 deny tcp destination-port eq 1900
```

rule 80 deny udp destination-port eq netbios-ns
rule 90 deny udp destination-port eq netbios-dgm
rule 100 deny udp destination-port eq netbios-ssn
rule 110 deny udp destination-port eq 445
rule 120 permit ip source 192.168.1.100 0
rule 1000 permit ip
#

包过滤 和 ip source guard 都是通过acl 实现的，先匹配上了包过滤 并执行了最后一条permit 动作，就不在匹配ipsg 绑定的规则了；

## 解决方法

去掉 rule 1000 permit ip，包过滤 只deny 匹配上规则的报文，即acl内添加的那些deny规则；匹配不上包过滤的话，会继续匹配ipsg 绑定的规则