# 某局点 某盒式交换机 包过滤不生效

ACL packet-filter 付军 2023-05-30 发表

## 问题描述

现场反馈配置了包过滤packet-filter不生效，配置了仍然能访问某IP地址

## 过程分析

查看设备涉及该问题的配置大致如下，现场在这些接口上的包过滤同时应用了一个IPv4高级ACL和一个二层ACL，二层的ACL优先级确实比较高，二层因为是匹配的mac，所以会优先转发，如果配置了rule permit，就会因为匹配上这个规则而不匹配其他的了，如果不配置，则是匹配不上，交换机缺省的动作也是转发，会进行其他规则的匹配

```
# interface GigabitEthernet1/0/1
 packet-filter mac 4001 inbound
 packet-filter 3001 inbound
 packet-filter mac 4001 outbound
#

#
acl mac 4001
 rule 1 deny dest-mac xxxx-xxxx-xxxx ffff-ffff-ffff
 rule 10 permit
#

#
acl advanced 3105
 rule 1 deny ip source xxx destination xxx
 rule 5 permit ip
#
```

## 解决方法

```
#
acl mac 4001
 rule 1 deny dest-mac xxxx-xxxx-xxxx ffff-ffff-ffff
 rule 10 permit     // 这条规则删了就行了
#
```