# S7006交换机端口下发ACL不生效问题处理案例

ACL　樊金帅　2019-02-25 发表

## 组网及说明

客户在GigabitEthernet3/0/34接口下调用qos policy禁止DHCP报文传输，但是下面的终端仍然能够正常获取地址，收集DHCP debug信息仍然有报文交互。

## 问题描述

```
#
interface GigabitEthernet3/0/34
 port link-mode bridge
 port access vlan 3
 stp edged-port enable
 qos apply policy policy_1 inbound
#
qos policy policy_1
 classifier classifier_1 behavior behavior_1
#
traffic classifier classifier_1 operator and
 if-match acl 3001
#
traffic behavior behavior_1
 filter deny
acl number 3001
 rule 10 permit tcp destination-port eq 67
 rule 15 permit tcp destination-port eq 68
 rule 20 permit udp destination-port eq bootps
 rule 25 permit udp destination-port eq bootpc
```

## 过程分析

通过查看终端网卡信息，发现仍可以正常获取地址


查看debug发现，dhcp报文正常交互

*Feb  1 15:05:43:644 2019 XDFE-JF-S7006-Core-01 DHCPR/7/DHCPR_DEBUG_PACKET:
From server to client (Server-group 1):
    Message type: reply
    Hardware type: 1, Hardware address length: 6
    Hops: 0, Transaction ID: 2252143997
    Seconds: 0, Broadcast flag: 1
    Client IP address: 0.0.0.0   Your IP address: 192.168.10.195
    Server IP address: 0.0.0.0   Relay agent IP address: 192.168.8.2
    Client hardware address: 0004-1d00-3b06
    Server host name: Not Configured, Boot file name: Not Configured
    DHCP message type: DHCP Ack

通过查看ACL3001底层信息，发现已经正常下发到硬件

Acl-Type MQC Port, Stage IFP, GroupPri 11, EntryID 270, Active

Health 1, PoolFree 0, PoolID 0, Prio_Mjr 518, Prio_Sub 14,Slice 11,SliceIdx 2

Policy policy_1, Classifier classifier_1, Behavior behavior_1

ACL GroupNo : 3001, RuleID : 20

Rule Match --------

Ports: 0x000000100, 0x01fffffff

IP protocol: udp

IP Type: Any IPv4 packet

L4 Dst Port: 67, 0xffff

Actions --------

Deny

========

Acl-Type MQC Port, Stage IFP, GroupPri 11, EntryID 271, Active

Health 1, PoolFree 0, PoolID 0, Prio_Mjr 518, Prio_Sub 14,Slice 11,SliceIdx 3

Policy policy_1, Classifier classifier_1, Behavior behavior_1

ACL GroupNo : 3001, RuleID : 25

Rule Match --------

Ports: 0x000000100, 0x01fffffff

IP protocol: udp

IP Type: Any IPv4 packet

L4 Dst Port: 68, 0xffff

Actions --------

Deny

## 解决方法

查看配置发现该设备为DHCP中继设备且配置了dhcp-snooping，这样的话DHCP报文会直接上CPU，因此无法被过滤
现场调整组网方式解决