

知 某局点105X ACL下发失败，资源提示不足

VLAN ACL packet-filter 李先福 2020-03-24 发表

组网及说明

不涉及

问题描述

客户发现在vlan if下发包过滤失败有如下报错

```
<GAZW-JIANGNINGFJ>-vlan-interface1\vlan 7
GAZW-JIANGNINGFJ>-vlan7 name deny-virus
GAZW-JIANGNINGFJ>-vlan7 int vlan7
GAZW-JIANGNINGFJ>-vlan-interface7 desc Xinghengguozh
GAZW-JIANGNINGFJ>-vlan-interface7 packet-filter name deny-virus inbound
GAZW-JIANGNINGFJ>-vlan-interface7 packet-filter name deny-virus outbound
Failed to apply 3rd Acl deny-virus to the outbound direction of interface vlan-interface7 on chassis 1 (slot 0, 2, 4), chassis 2 (slot 0, 2, 4).
```

过程分析

(1) 查看设备的acl资源，发现acl资源已经差不多用完

```
<GAZW-JIANGNINGFJ>-dis qos-acl resource
Interfaces: XGE1/0/0/1 to XGE1/0/0/16 (chassis 1 slot 0)
-----
Type          Total    Reserved  Configured  Remaining  Usage
-----
VFP ACL       1024     768        0            256        75%
IFP ACL       2048     768        1080         200        90%
IFP Meter     1024     512        0            512        50%
IFP Counter   1024     384        0            640        37%
EFP ACL       1024     0          1020         4          99%
EFP Meter     512      0          0            512        0%
EFP Counter   512      0          0            512        0%
```

(2) 查看客户的acl配置和包过滤应用

```
#
acl advanced name deny-virus
step 10
rule 0 deny tcp destination-port eq 4899
rule 1 deny udp destination-port eq 4899
rule 2 deny udp destination-port eq 22
rule 20 deny tcp destination-port eq 9996
rule 30 deny tcp destination-port eq 135
rule 40 deny tcp destination-port eq 136
rule 50 deny tcp destination-port eq 137
rule 60 deny tcp destination-port eq 138
rule 70 deny tcp destination-port eq 139
rule 80 deny tcp destination-port eq 445
rule 90 deny udp destination-port eq 135
rule 100 deny udp destination-port eq 2425
rule 110 deny tcp destination-port eq 2425
rule 120 deny udp destination-port eq 136
rule 130 deny udp destination-port eq netbios-ns
rule 140 deny udp destination-port eq netbios-dgm
rule 150 deny udp destination-port eq netbios-ssn
rule 160 deny udp destination-port eq 445
rule 170 deny udp destination-port eq 1434
rule 180 permit ip
##共19条rule
```

共在54个vlan接口下发这个包过滤。设备在底层会占用54份包过滤的acl资源，也就是 $54 \times 19 = 1026$ ，与客户查看acl资源占用情况差不多。

(3) 建议改成全局下发包过滤，这样设备只会下发一份底层资源，只占用19份acl资源，从而节约acl资源。

解决方法

将包过滤在全局下发，而不在单个vlan接口逐个下发。