某局点 S7003X vlan下发包过滤出方向不生效问题

ACL packet-filter **姚智祥** 2022-06-22 发表

组网及说明

无

告警信息

无

问题描述

设备及版本：S7003X　　Release 7743P04

问题描述：

现场设备做网关，测试流为10.1.3.39------10.1.130.33，在ping通的情况下，发现在出入方向的vlan虚接口下分别调用包过滤时，出方向不生效。

测试结果如下：

在Vlan-interface30接口下配置packet-filter 3020 inbound生效

配置packet-filter 3010 outbound不生效

在Vlan-interface330接口下配置packet-filter 3010 inbound生效

配置packet-filter 3020 outbound不生效

过程分析

1.看设备没有acl不足的情况，也没有冲突的其他acl调用

```
Advanced IPv4 ACL 3010, 2 rules,
ACL's step is 5, start ID is 0
rule 0 deny ip source 10.1.130.0 0.0.0.255 destination 10.1.3.39 0
rule 5 permit ip

Advanced IPv4 ACL 3020, 2 rules,
ACL's step is 5, start ID is 0
rule 0 deny ip source 10.1.3.39 0 destination 10.1.130.0 0.0.0.255
rule 5 permit ip

[XC-B-CORE-S7003X-03]dis arp 10.1.3.39
  Type: S-Static    D-Dynamic    O-Openflow   R-Rule   I-Invalid
IP address      MAC address    VLAN/VSI name Interface             Aging Type
10.1.3.39       988d-4613-20bd 30            BAGG11                1036  D

[XC-B-CORE-S7003X-03]dis cur int vlan 30
#
interface Vlan-interface30
description 无线
ip address 10.1.3.1 255.255.255.0
dhcp select relay
dhcp relay server-address 10.1.120.50
#

[XC-B-CORE-S7003X-03]dis arp 10.1.130.33
  Type: S-Static    D-Dynamic    O-Openflow   R-Rule   I-Invalid
IP address      MAC address    VLAN/VSI name Interface             Aging Type
10.1.130.33     1234-5678-90ab 330           BAGG17                1082  D

[XC-B-CORE-S7003X-03]dis cur int vlan 330
#
interface Vlan-interface330
description 闅旂 缃戞
ip address 10.1.130.1 255.255.255.0
dhcp select relay
dhcp relay server-address 10.1.120.50
#

[XC-B-CORE-S7003X-03]dis qos-acl resource
Interfaces: GE0/0/1 to GE0/0/16, XGE0/0/17 to XGE0/0/28 (slot 0)
---------------------------------------------------------------------
Type            Total      Reserved   Configured Remaining  Usage
---------------------------------------------------------------------
IGS ACL         8192       200        0          7992       2%
EGS ACL         1536       0          4          1532       0%
IGS Counter     2044       100        0          1944       4%
EGS Counter     511        0          0          511        0%
IGS Meter       8192       100        0          8092       1%
EGS Meter       2048       0          0          2048       0%
IMeter Counter  4095       300        0          3795       7%
EMeter Counter  4095       0          0          4095       0%

Interfaces: GE1/0/1 to GE1/0/24, XGE1/0/25 to XGE1/0/40 (slot 1)
---------------------------------------------------------------------
Type            Total      Reserved   Configured Remaining  Usage
---------------------------------------------------------------------
IGS ACL         8192       200        0          7992       2%
EGS ACL         1536       0          4          1532       0%
IGS Counter     2044       100        0          1944       4%
EGS Counter     511        0          0          511        0%
```

IGS Meter	8192	100	0	8092	1%
EGS Meter	2048	0	0	2048	0%
IMeter Counter	4095	300	0	3795	7%
EMeter Counter	4095	0	0	4095	0%

经确认，该设备存在以下限制：vlan下发包过滤时，缺省情况下仅过滤三层转发的报文。会通过匹配vlan id和三层转发标志来区分vlan虚接口，对于跨芯片、跨板的三层转发流量，在出芯片、出口板上不做三层转发，因此没带三层转发标志，导致ACL无法匹配。可在vlan下配置packet-filter filter all，配置后下发acl表项时三层转发标志不会下发，二层、三层报文都可以匹配。

解决方法

可在vlan下同时配置packet-filter filter all，配置后下发acl表项时三层转发标志不会下发，二层、三层报文都可以匹配。