



某局点 S12508F-AF 流策略下发失败

ACL

QoS

packet-filter

张正强

2021-09-22 发表

组网及说明

不涉及

问题描述

- 接口下应用qos流策略功能进行流量过滤，发现三层流量互访符合过滤策略规划，但是二层流量互访却出现了中断问题；按照网段规划，39.136.10.X能够匹配上acl 3011中的rule 365然后被permit放通，但是业务实测二层互访不通；
- 但是接口下应用packet-filter就不会导致二层流量互访不通；
- 不配置流策略的情况下，也没有影响；

```
[H3C-Bridge-Aggregation1]dis qos policy i o
Interface: Bridge-Aggregation1
Direction: Outbound
Policy: aaa
Classifier: aaa1
  Operator: AND
  Rule(s) :
    If-match acl 3011
    Behavior: permit
    Filter enable: Permit
Classifier: aaa2
  Operator: AND
  Rule(s) :
    If-match acl 3013
    Behavior: permit
    Filter enable: Permit
Classifier: aaa3
  Operator: AND
  Rule(s) :
    If-match acl 3012
    Behavior: deny
    Filter enable: Deny
```

过程分析

1. 官网acl章节中有如下的使用限制说明，qos filter和packet-filter在使用时，对于二层转发的出现流量是匹配不上对应的acl rule的；即bagg1出方向上应用的qos filter，39.136.10.X网段的流量是匹配不上acl 3011 rule 365的；

1. 配置限制和指导

当ACL用于QoS策略的流分类或用于报文过滤功能时：

- 若报文过滤功能应用于出方向，规则不支持配置vpn-instance参数。
- 若QoS策略或报文过滤功能应用于出方向：
 - 对于上送CPU后的报文、进行二层转发的报文和进行三层转发的报文，IPv4基本ACL规则rule [rule-id] { deny | permit } { object-group address-group-name | source { source-address source-wildcard | any } | vpn-instance vpn-instance-name }仅支持匹配进行三层转发的报文。

2. Bagg1应用的qos filter的第三个cb对中acl 3012下发了rule 5 deny ip，这条规则在底层会下发三条deny规则，一条用于deny ipv4_uc、即ipv4单播流量，一条deny ipv4_mc、即ipv4组播，一条ipv4_any、即任意ipv4流量；bagg1上来二层互访的39.136.10.X的流量，能够匹配上ipv4_any这一条，然后被deny掉，因此二层流量不通；

```
=====
Acl-Type MQC BAGG, Stage EFP, OuterPort, Installed, Active
L2 PROGRAM : Prio Mjr/Sub 4/411, Group 5 [0], enRtnHealth 1, Entry 323, Mdc 1
PolicyID 100, CBMapID 2, ClassID 101, BehaviorID 101 [OUT]
ACL GroupNo : 3012, RuleID : 5 V4v6 1
Rule Match -----
    Port Class: 0xffffffff, 0xffffffff Port ClassID:0x4, 0x7c |
stPbmp=0x0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
,
stPbmpMask=0x0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000
    IP Type: Any IPv4 packet EFP Arad Don't Set
    DST TRUNK: 2 Mask 255
    Not mirror copy
Actions -----
    Deny
L2 PROGRAM : Bank 4 Location 517 HIT(read-clear): YES
=====
```

3. Vlan-int下应用packet-filter acl 3011，最后有一条deny ip，这个deny在底层只会下一条ipv4_uc的规则，这个规则只能用于匹配三层单播流量，因此匹配不上39.136.10.X网段的二层互访流量；但是包过滤缺省是放通的，因此在vlan-int下应用报过没有deny掉二层互访的业务；

```
=====
Acl-Type PktFilter IP on VRF, Stage EFP, OuterPort, Installed, Active
L2 PROGRAM : Prio Mjr/Sub 8/1576992762, Group 6 [0], enRtnHealth 1, Entry 169, Mdc 1
ACL GroupNo : 3458, RuleID : 5 V4v6 1
Rule Match -----
    Port Class: 0xffffffff, 0xffffffff Port ClassID:0x4, 0x7c |
stPbmp=0x0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
,
stPbmpMask=0x0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000
    IP Type: Any IPv4 packet EFP Arad Don't Set
    Not mirror copy
    Forwarding Type: ipv4_uc
    Vfi: 1234, VfiMask 0xffff Qualify Vpn
Actions -----
    Deny
```

L2 PROGRAM : Bank 8 Location 1 HIT(read-clear): NO

解决方法

1. 在流量入方向上使用qos流策略，避开上述的acl出方向的使用限制；
2. 在对应的vlan-int应用packet-filter

