某局点S12508 PBR不生效故障案例分析

ACL 策略路由 **胡晓东** 2020-02-28 发表

组网及说明

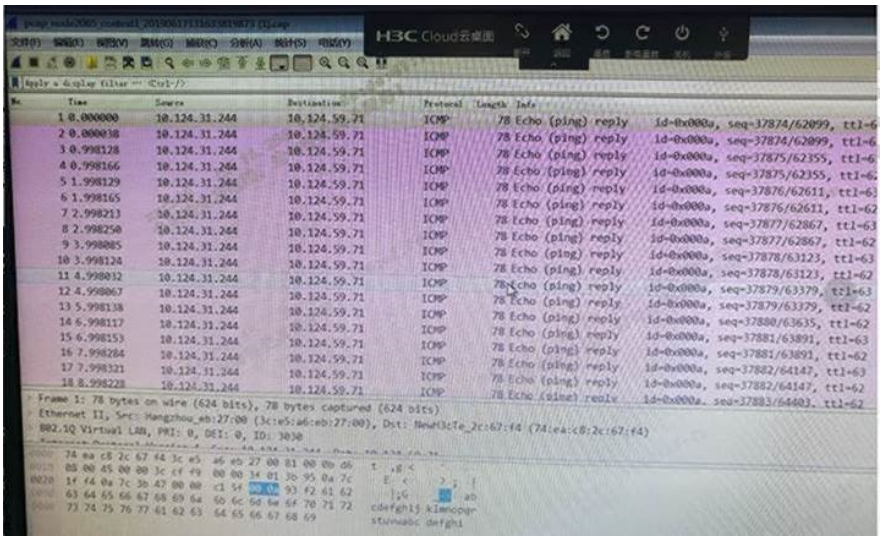
设备型号：S12508

设备版本: 1728P02

问题描述

故障现象具体为：10.124.59.71访问10.124.31.244，发现去的流量没匹配pbr上防火墙，31.244回来的流量匹配了pbr。59.71访问31.2的流量能匹配上pbr。

图为10.124.59.71访问10.124.31.244tracert信息，12508引流10.124.59.0前半个C地址至防火墙。



过程分析

1）查看诊断和配置信息发现，不生效的PBR下发在VLAN59中：

```
#
interface Vlan-interface59
ip address 10.124.59.250 255.255.255.0
ip policy-based-route shangxing
#
policy-based-route shangxing permit node 100
  if-match acl 3030
  apply ip-address next-hop 10.124.52.194
#
acl number 3030
description Server_Fw_shangxing
rule 1000 permit ip source 10.124.59.0 0.0.0.127
rule 2000 permit ip destination 10.124.59.0 0.0.0.127
```

2）该设备匹配规则的优先级是全局>端口>vlan，由于入端口下配置了包过滤和mqc，进来的流量会优先匹配包过滤和mqc,无法匹配PBR的规则，从而导致PBR不生效的现象。

```
#
interface Ten-GigabitEthernet1/2/0/27
port link-mode bridge
description To_C10-C20_H3C5830_000231
port link-type trunk
port trunk permit vlan 1 to 299
packet-filter 3123 inbound
packet-filter 3123 outbound
qos apply policy bd inbound
qos apply policy test outbound
mirroring-group 1 mirroring-port both
port link-aggregation group 27
#
#
interface Ten-GigabitEthernet2/2/0/27
```

port link-mode bridge
description To_C10-C20_H3C5830_000231
port link-type trunk
port trunk permit vlan 1 to 299
packet-filter 3123 inbound
packet-filter 3123 outbound
qos apply policy bd inbound
qos apply policy test outbound
mirroring-group 2 mirroring-port both
port link-aggregation group 27

#
packet-filter 3123 inbound
packet-filter 3123 outbound
qos apply policy bd inbound
#
acl number 3123
description bing'du'fang'fan
rule 3123 permit ip
acl number 3334
rule 2 permit ip

解决方法

修改入端口的规则，以保证PBR的流量匹配不到端口下的规则即可