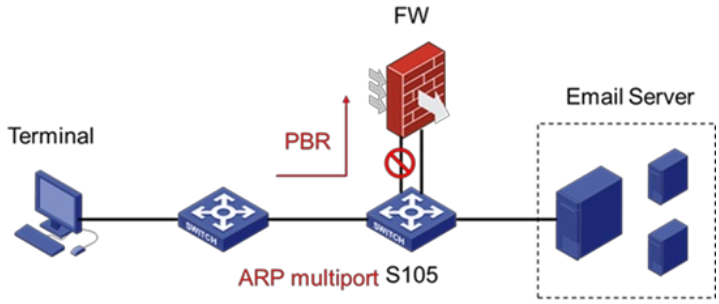
某局点S10506X交换机配置多端口ARP功能后不生效

ARP 董智敏 2022-02-28 发表

组网及说明

现场组网如下S105上行通过配置多端口arp和邮件服务器集群对接，终端和邮件服务器互访的流量会通过pbr绕行到防火墙



问题描述

现场发现S10506X上配置多端口arp后发现终端无法ping通邮件服务器的ip地址，去掉“arp multiport 虚IP 组播MAC VLAN ID”命令后可以互通，故障时流统确认是丢在我们设备出方向。

过程分析

经过排查，发现当配置“arp multiport *虚IP 组播MAC VLAN ID*”命令后，终端访问邮件服务器的报文在进入S105后并没有从任何接口发送出去，表明报文在S105内部被丢弃。进一步排查，发现终端访问邮件服务器的报文在进入S105后首先需要通过PBR引流到旁挂的一台防火墙，防火墙送回S105再通过路由表进行转发。

设备上多端口arp的实现依赖于底层下发acl规则，而pbr也是通过acl规则实现，多端口arp的acl优先级高于pbr。因此，当终端过来的报文同时满足pbr和多端口arp的acl匹配规则时会优先被多端口arp匹配走，从而报文无法正常从S105发送到防火墙。

解决方法

可以采用vpn路由方式让设备流量先到FW，然后在从FW返回来进行arp转发。
流量从入vlan 10(绑定vpna)进入时，在vpna内查路由表转发到FW,FW更换vlan 21(绑定vpnb)后再返回到设备上，此时流量在vpnb内查询多端口arp进行转发。

参考配置:

```
ip vpn-instance vpna
 route-distinguisher 1.1.1.1:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
#
ip vpn-instance vpnb
 route-distinguisher 1.1.1.1:2
 vpn-target 200:1 import-extcommunity
 vpn-target 200:1 export-extcommunity
#

#
interface Vlan-interface10
 ip binding vpn-instance vpna
 ip address 10.0.0.1 255.0.0.0
#
interface Vlan-interface20
 ip binding vpn-instance vpna
 ip address 20.0.0.1 255.0.0.0
#
interface Vlan-interface21
 ip binding vpn-instance vpnb
 ip address 21.0.0.1 255.0.0.0
#
interface Vlan-interface30
 ip binding vpn-instance vpnb
 ip address 30.0.0.1 255.0.0.0


#
 ip route-static vpn-instance vpna 0.0.0.0 0 20.0.0.2
#
 mac-address multicast 03bf-ac10-010d interface Ten-GigabitEthernet1/0/30 Ten-
GigabitEthernet1/0/32 vlan
30
 arp multiport 30.0.0.2 03bf-ac10-010d 30 vpn-instance
vpnb
#
```