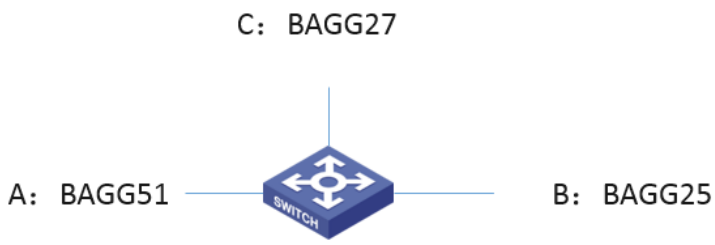
某局点二层泛洪流量变成三层转发问题分析

二层转发 IP转发 VLAN 曾嘉明 2020-02-27 发表

组网及说明



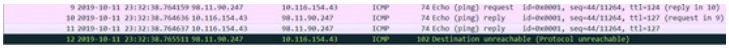
问题描述

如上图所示，A去ping B，然后B上装了一个软件，会把B收到和发出的所有报文都封装到一个特定的4013的vlan，然后在vlan内泛洪给C，但是测试发现，request报文可以泛洪给C，但是response报文没法泛洪给C，反而是发给了A。

最终定位是因为在S6800上，为了节约表项资源，并不会去查找vlan信息，而是先查找路由表，然后就转发走了，如果要开启vlan检查，就要给三层虚接口配置手工MAC。

过程分析

1、查看51口的抓包，发现竟然有两个response报文，还有一个unreachable报文。

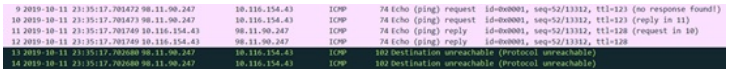


51口明明没有放通这个用于泛洪的4013，所以不应该有第二个reply报文，同时那个unreachable报文也很奇怪。

2、查看27口抓包：

只有request报文，没有response报文，反而也多了一个unreachable报文。

3、查看25口的抓包：



两个request报文，两个response报文，正常，但是也有两个unreachable报文，异常。

结合整个流程来看，可以确定，是由于25口进来的·response报文，没有在vlan4013里泛洪，反而是查表转发到了51口，但是51口又没有发出它的request报文，所以认为是目的不可达的，所以就回了一个unreachable报文给25口，然后25口又把这个unreachable报文泛洪给了27口，导致出现这种27口收不到response的镜像报文，反而收到一个unreachable报文。

所以最终需要找到的原因就是25口镜像出来的response报文为什么没有泛洪，反而查表转发了。

最终定位是由于S6800的实现机制问题，报文进来后默认不区分VLAN，就直接查表，可以通过下述命令查看：

[S6800-probe]bcm s 2 c 0 d/chg/my_station_tcam
MY_STATION_TCAM.ipipe0[11]: <VALID=1,MPLS_TERMINATION_ALLOWED=1,MASK=0x00000000ffffffffffff,MAC_ADDR_MASK=0xffffffffffff,MAC_ADDR=0x9ce89572832a,KEY=0x000000009ce89572832a,IPV6_TERMINATION_ALLOWED=1,IPV4_TERMINATION_ALLOWED=1,DATA=0x3a,ARP_RARP_TERMINATION_ALLOWED=1>

MY_STATION_TCAM.ipipe0[14]:
<VLAN_ID_MASK=0xfff,VLAN_ID=2,VFI_ID_MASK=0xfff,VFI_ID=2,VALID=1,MPLS_TERMINATION_ALLOWED=1,MASK=0x00000fffffffffffffff,MAC_ADDR_MASK=0xffffffffffff,MAC_ADDR=0x9c8e95728331,KEY=0x000000029c8e95728331,IPV6_TERMINATION_ALLOWED=1,IPV4_TERMINATION_ALLOWED=1,DATA=0x3a,ARP_RARP_TERMINATION_ALLOWED=1>

可以看到，手动修改了这个interface vlan下的mac时候，就会产生这个加粗的字段，这个字段代表的含义就是需要进行vlan的匹配，如果匹配不成功就不会查表，匹配成功才能查表转发。

解决方法

网段B对应的网关下绑定一个MAC地址，地址无要求，与现有设备上的MAC不冲突即可，这样就可以开启设备的VLAN检查功能。