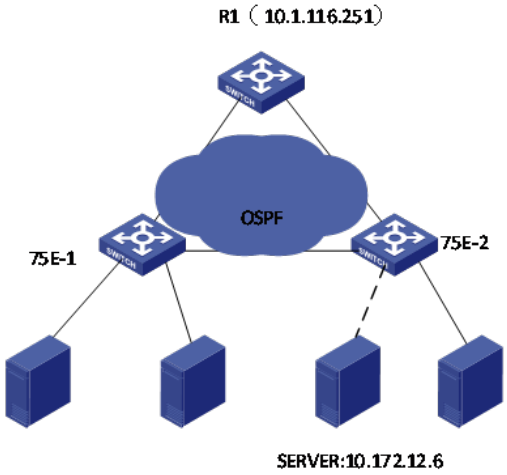
# 某局点75E三层转发变广播的问题分析

ARP IGMP PIM 郭威 2014-07-21 发表

某局点75E三层转发变广播的问题分析

**一、 组网：**




R1与S75E-1与S75E-2之间是三层，通过OSPF路由互联。两台S75E做为网关，直连接入数台服务器。其中虚线所示的服务器表示曾经存在的服务器，现在已经移开。

**二、 问题描述：**

现在远端R1（10.1.116.251）的数据发往10.172.12.6这个服务器的地址，而这个地址所对应的服务器已经撤去，在75E-1与75E-2上均不存在。正常情况下这个报文应该丢弃，但是这个报文却在S75E-2下面的其他服务器上收到了该报文，而S75E-1下面的服务器未收到。因此怀疑S75E-2的三层转发出现了问题。

**三、 过程分析：**

1、 首先通过在S75E-2下面的服务器上抓包，确认问题现象。

在S75E-2上没有找到目的地址为10.172.12.6的ARP表项，而该框G5/0/1、G5/0/2下接的服务器的地址分别是10.172.12.36和10.172.12.24，在服务器上抓包，抓到了很多目的地址为10.172.12.6的报文。进一步发现G5/0/1与G5/0/2处于同一VLAN。

```
#
interface GigabitEthernet5/0/1
 port link-mode bridge
 port access vlan 150
 #
 interface GigabitEthernet5/0/2
 port link-mode bridge
 port access vlan 150
#
```

经确认在VLAN 150内的服务器上均收到了目的地址为10.172.12.6的报文，因此怀疑报文在VLAN 150内进行了泛洪处理。

2、 在S75E-2上通过流量统计确认报文的来源。

由于怀疑在VLAN内进行了泛洪处理，因此怀疑报文并非是S75E-2三层转发导致的，而是有可能从其他属于VLAN 150内的接口进入的，因为没有10.172.12.6的ARP表项而导致泛洪处理。在设备上进行流量统计，查看报文是从哪个接口进来的。

```
#
acl number 3000
 rule 0 permit ip source 10.1.116.251 0 destination 10.172.12.8 0
traffic classifier acc
   if-match acl 3000
traffic behavior acc
   accounting
```

qos policy acc

classifier acc behavior acc

#

在所有放通VLAN 150的接口下做了双向的流量统计，最终发现流量是通过S75E-1互联接口G2/0/47进入到S75E-2上的。进一步与远端R1确认，流量并非直接传输到S75E-2。因此可以进一步确定S75E-2的三层转发没有问题，是由于流量从S75E-1通过聚合口到达S75E-2，而S75E-2没有该ARP，故在VLAN 150内广播。

#

interface GigabitEthernet2/0/47

port link-mode bridge

port link-type trunk

port trunk permit vlan 1 to 104 106 to 4094

3、 确认S75E-1为何会将该报文转发至S75E-2。

此时在S75E-1上发现存在该IP的ARP静态短绑定

arp static 10.172.12.6 0050-5647-23eb

现场发现将该ARP静态绑定去除后，问题解决，而将该ARP表项重新静态绑定时，问题不复现。

在S75E-1上查看ARP表项，看到删除前该ARP表项为静态绑定

10.172.12.6 0050-5647-23eb 150 GE5/0/35 N/A S

删除后重新绑定，则为

10.172.12.6 0050-5647-23eb N/A N/A N/A S

而G5/0/35是S75E-1上与S75E-2互联的接口。询问过现场10.172.12.6这个地址曾经是接在S75E-2上的。

由此问题确认：

(a) 最初：

10.172.12.6的服务器接在S75E-2上，在S75E-1配置了该ARP的静态短绑定，此时设备S75E-1并不知道其所属VLAN与接口信息，因此全是N/A，而当S75E-2通过互联口从S75E-1学习到了ARP表项后，下发到硬件底层的信息变成了ARP长绑定，即包含了VLAN 与接口信息。S75E-1上应该是

10.172.12.6 0050-5647-23eb 150 GE5/0/35 N/A S

(b)然后：

10.172.12.6的服务器从S75E-2上移除，S75E-2上清除其ARP表项。而对于S75E-1来说，由于下发到底层的是静态ARP，从而不会老化；而S75E间的互连口一直UP，因此不会清除ARP表项，而S75E-1又并未从其他接口学习到10.172.12.6的ARP表项，因此不会刷新底层的表项。

(c)最后：

当访问10.172.12.6的三层流量到达S75E-1上后，查找到有相应的ARP，便将流量从互联口传输到S75E-2上，而此时S75E-2上VLAN 150内没有相应的ARP表项，于是在VLAN 150内进行了泛红处理。

**四、 解决方法：**

建议现场重新下发ARP绑定，或者取消ARP绑定。