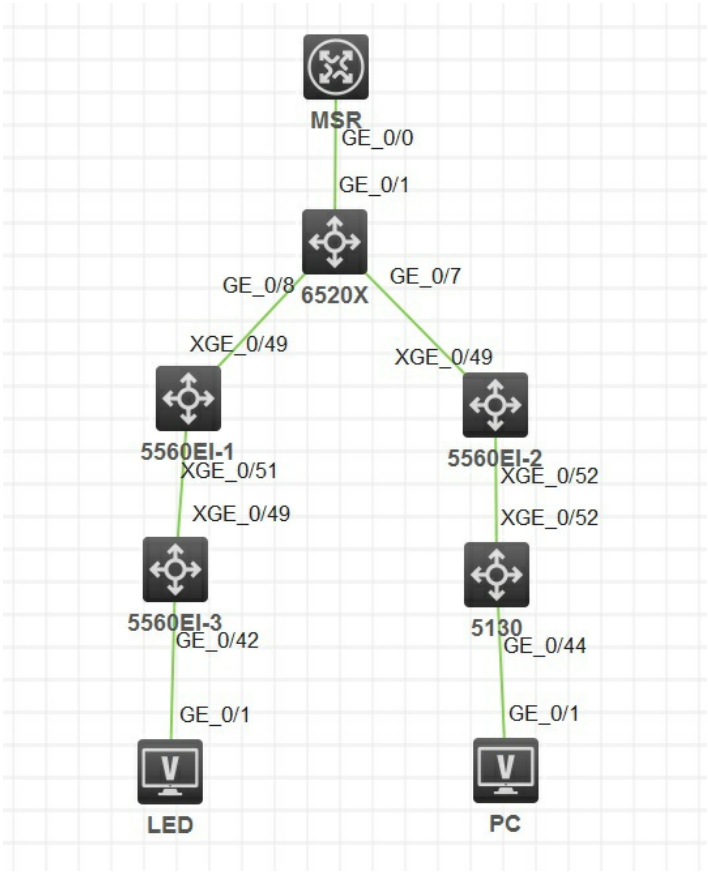
某局点S6520X-30QC-EI 疑似端口隔离异常问题

二层端口隔离 DHCP Snooping ARP **折锐鹏** 2019-12-10 发表

组网及说明



问题描述

某局点遇到如下问题。

组网中LED屏幕（MAC地址0004-a301-0009，IP地址是10.100.0.59）无法同PC通信。LED上接S5560EI-3的42口，PC接接入交换机5130的44口。5560E和6520X上下行口都配置了端口隔离。设备网关在MSR上，在网关上配置了arp代理功能。但是有一个故障现象是在PC上学习到的LED的ARP信息MAC是LED的（原理上应该是学习到网关MAC地址），从而导致报文目的mac异常会出现无法通信的问题。

注：业务通信使用vlan 3301，对应接口都放通了该vlan

测试抓包：

在S5560EI-2的42口（设备上的一个未使用端口）上用自己PC（IP地址是10.100.150.124，MAC地址是f430-b9d2-27dc）模拟管理服务器抓包，发现回包的arp是LED屏。如果开启了端口隔离，照理来说PC学习到的应该是网关的MAC地址。

过程分析

最先怀疑是有连线私接导致对应的两个设备直连，所以从未隔离的接口把arp报文广播过去了，于是看了下mac漂移，也没有看到对应到的vlan有漂移的记录。

然后进行远程发现在5560EI-2上起了一个int vlan 3301，并配置了一个同网段的静态ip地址，发现并不会学习到LED屏幕的arp信息，学习的是网关的arp，故障未复现。之后将int vlan 3301改为dhcp alloc动态获取地址，问题复现了。

在6520X上开启debug rxtx source-mac 查询对应的arp，发现arp报文被单播发送出去了。

这是因为7口和8口上使能了dhcp snooping、端口隔离，所在vlan使能arp detection的情况下。从7口上来的arp广播报文会上送平台处理，平台会基于DHCP Snooping表项进行检查，并根据表项中记录的出端口将报文转发出去，不再广播，所以直接在7口下面的终端上学习到了arp，报文没有上送到上联的arp代理设备。

6520X的7口和8口配置如下

```
#
interface Ten-GigabitEthernet1/0/7
 port link-mode bridge
 description hdl2lou
 port link-type trunk
 port trunk permit vlan 1 to 2 18 21 to 22 25 33 64 80 3301 3500
 port-isolate enable group 1
 undo stp enable
```

```
 dhcp snooping binding record
 dhcp snooping check mac-address
#
interface Ten-GigabitEthernet1/0/8
 port link-mode bridge
 description qzl8lou
 port link-type trunk
 port trunk permit vlan 1 to 2 7 18 21 to 22 25 31 33 64 80 3301
 port trunk permit vlan 3306 3350 3401 3500 to 3501 3505
 port-isolate enable group 1
 undo stp enable
 dhcp snooping binding record
 dhcp snooping check mac-address
#
```

解决方法

通过配置arp detection port-match-ignore，忽略端口检查，arp报文不通过dhcp snooping的表项转发，而是将报文广播出去，这样就可以到代理设备了。