某局点F5030-D冗余切换异常

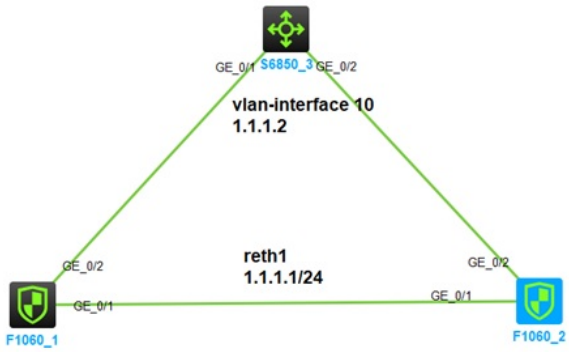
冗余组 备份组 冗余口 孔德飞 2023-07-23 发表

组网及说明

组网如下：

简化组网如下：

FW1与FW2冗余主备，冗余的主在FW1，IRF的主在FW2



告警信息

不涉及

问题描述

故障现象，当冗余的主在FW1上的时候，FW1 以自己的源地址1.1.1.1 ping1.1.1.2的时候，可以通
此时，将FW1的上行口shutdown，此时冗余的主切换到FW2，然后FW1上行口undo shutdown，等待1分钟，当冗余组的主切换到FW1上的时候，此时FW1以自己的源地址1.1.1.1 pinig 1.1.1.2不通

过程分析

问题分析过程

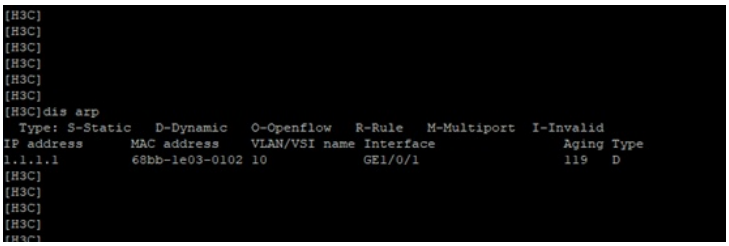
排查发现，上行SW配置了如下命令

arp active-ack enable，该命令是设备主动ARP的主动确认功能主要应用于网关设备，防止攻击者仿冒用户欺骗网关设备。

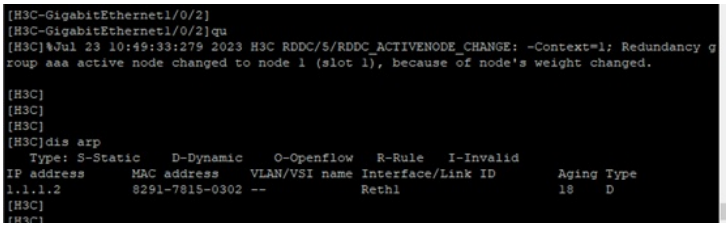
即在SW自身有ARP的前提下，会确认ARP响应报文的入接口与自己学习到的是否一致，不一致则认为是欺骗。

模拟器复现如下：

1. 将FW1的上行口g1/0/2关闭，此时FW1可以ping通1.1.1.2，此时在SW上查看1.1.1.1的ARP，发现ARP的接口刷新为g1/0/2基于FW2相连的接口，因为此时是down掉了物理接口，所以此时SW的原本接口g1/0/1的ARP会消失，接口都down了

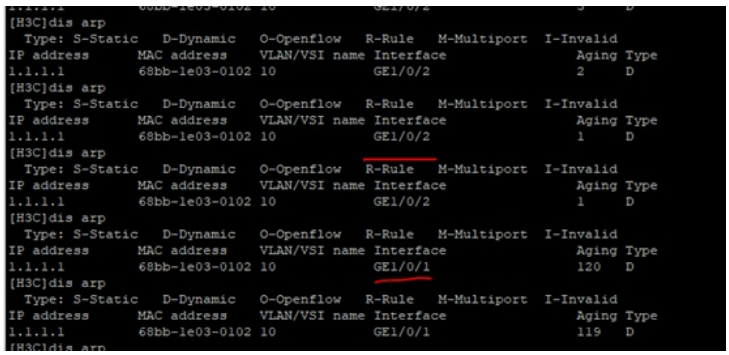


2 将FW1的上行口g1/0/2 undo shutdown，等待1分钟，FW1的冗余主已经回切抢占



为了方便观察，已经将SW的ARP动态老化时间手工更改为2分钟，即120秒

SW上立刻查看ARP，发现ARP接口未更新，当SW上的ARP老化之后，SW上的ARP接口已经更新为g1/0/1.



解决方法

问题解决方案

将FW上行SW上的arp active-ack enable给去掉