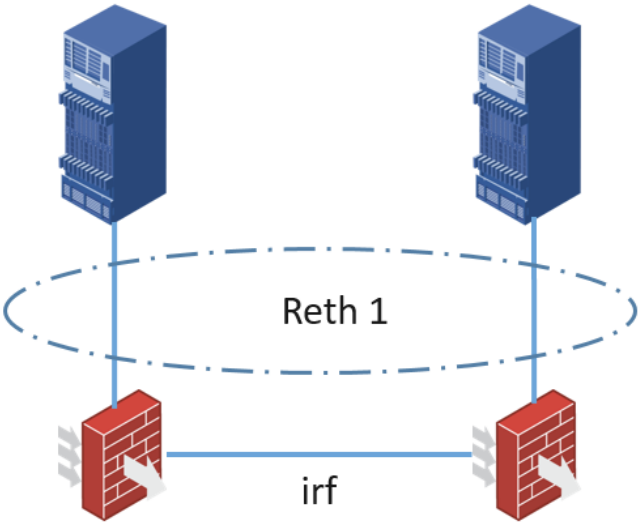
某局点F5080（V7）防火墙冗余组切换后无法ping通上行交换机互连接口地址

冗余组 冗余口 ARP 产品特性 **刘诚** 2021-04-29 发表

组网及说明



组网说明：防火墙堆叠部署，上行两台交换机防火墙主备单独互连（不做irf），交换机与防火墙互连接口为三层口，且两个接口ip地址一样，对接防火墙reth1口。左边防火墙为主，右边防火墙为备，左边交换机称为A，右边交换机称为B。

问题描述

现场反馈对防火墙进行冗余组切换时，从主防火墙切到备防火墙，在防火墙上ping B与reth 1互连的接口地址不通，需要在防火墙上reset arp all或者等5分钟才能ping通；从备防火墙切到主防火墙，在防火墙上可以直接ping A与reth 1互连的接口地址。

过程分析

经过实验室测试：

倒换前，冗余组在主框，在防火墙上长ping：

```
dis redundancy group
Redundancy group 1 (ID 1):
  Node ID      Chassis       Priority   Status        Track weight
  1            Chassis1      90         Primary       255
  2            Chassis2      10         Secondary     255

Preempt delay time remained     : 0    min
Preempt delay timer setting     : 1    min
Remaining hold-down time        : 0    sec
Hold-down timer setting         : 1    sec
Manual switchover request       : No

Member interfaces:
    Reth5
Node 1:
  Track info:
    Track    Status          Reduced weight     Interface
      11       Positive         255                XGE1/3/0/1
Node 2:
  Track info:
    Track    Status          Reduced weight     Interface
    21       Positive         255                XGE2/3/0/1
```

通过shut XGE 1/3/0/1进行倒换后，冗余组切换到备上，此时测试长ping丢一个包。//丢一个包，与现场ping不通不一致

```
56 bytes from 70.1.1.2: icmp_seq=150 ttl=255 time=0.527 ms
56 bytes from 70.1.1.2: icmp_seq=151 ttl=255 time=0.548 ms
56 bytes from 70.1.1.2: icmp_seq=152 ttl=255 time=0.791 ms
56 bytes from 70.1.1.2: icmp_seq=153 ttl=255 time=0.541 ms
Request time out
56 bytes from 70.1.1.2: icmp_seq=155 ttl=255 time=1.016 ms
56 bytes from 70.1.1.2: icmp_seq=156 ttl=255 time=0.649 ms
56 bytes from 70.1.1.2: icmp_seq=157 ttl=255 time=0.559 ms
56 bytes from 70.1.1.2: icmp_seq=158 ttl=255 time=0.573 ms

dis redundancy group
Redundancy group 1 (ID 1):
  Node ID      Chassis       Priority   Status        Track weight
  1            Chassis1      90         Secondary     0
  2            Chassis2      10         Primary       255

Preempt delay time remained     : 0    min
Preempt delay timer setting     : 1    min
Remaining hold-down time        : 0    sec
Hold-down timer setting         : 1    sec
Manual switchover request       : Yes

Member interfaces:
    Reth5

Node 1:
  Track info:
    Track    Status          Reduced weight     Interface
    11       Negative         255                XGE1/3/0/1
Node 2:
  Track info:
```

Track Status Reduced weight Interface
21 Positive 255 XGE2/3/0/1

解决方法

shut XGE 1/3/0/1之后，冗余组回切，回切过程中未丢包。//回切不丢包，与现场描述一致

根据测试的结果分析 因为防火墙上是reth口，reth为逻辑口，当业务在主墙上时，防火墙学到的arp中mac表象为核心1上的mac，当业务切换至备墙后，由于arp还未老化，对与防火墙而言，arp表象里的mac还是核心1上的mac，发送的报文目的mac还是核心1的mac，这样报文到达核心2后，由于目的mac错误，核心会将报文丢弃。核心上配置免费arp后，核心定时发送免费arp告知防火墙核心mac的变化情况，使防火墙能够及时更新arp表象，用正确的mac去封装报文。这样切换后防火墙上的arp表象能及时刷新为正确的表象，倒换也就正常。

Redundancy group 1 (ID 1)
Node ID Chassis Priority Status Track weight
1 Chassis1 90 Secondary 255
2 Chassis2 10 Primary 255
Preempt delay time remained : 1 min
Preempt delay timer setting : 1 min
Remaining hold-down time : 0 sec
Hold-down timer setting : 1 sec
Manual switchover request : No
Manual switchover times : 0
Failure times : 5
Node 1:
Track info:
Track Status Reduced weight Interface
11 Positive 255 XGE1/3/0/1
Node 2:
Track info:
Track Status Reduced weight Interface
21 Positive 255 XGE2/3/0/1

实验环境测试，在备切回主的时候，对端设备会回一个免费arp给防火墙设备，所以回切的基本不丢包。

*Apr 24 15:56:48:990 2021 F1070 ARP/7/ARP_SEND: -COntext=1; Sent an ARP message, operation: 1, sender MAC: 3c8c-40b4-0921, sender IP: 70.1.1.1, target MAC: 0000-0000-0000, target IP: 70.1.1.1
*Apr 24 15:56:48:990 2021 F1070 ARP/7/ARP_SEND: -COntext=1; Sent an ARP message, operation: 1, sender MAC: 3c8c-40b4-0921, sender IP: 70.1.1.1, target MAC: 0000-0000-0000, target IP: 70.1.1.1
*Apr 24 15:56:50:990 2021 F1070 ARP/7/ARP_SEND: -COntext=1; Sent an ARP message, operation: 1, sender MAC: 3c8c-40b4-0921, sender IP: 70.1.1.1, target MAC: 0000-0000-0000, target IP: 70.1.1.1
*Apr 24 15:56:51:453 2021 F1070 ARP/7/ARP_RCV: -COntext=1; Received an ARP message, operation: 1, sender MAC: 9023-04c0-0633, sender IP: 70.1.1.2, target MAC: 0000-0000-0000, target IP: 70.1.1.2
*Apr 24 15:56:51:990 2021 F1070 ARP/7/ARP_SEND: -COntext=1; Sent an ARP message, operation: 1, sender MAC: 3c8c-40b4-0921, sender IP: 70.1.1.1, target MAC: 0000-0000-0000, target IP: 70.1.1.1

2.1.2 arp send-gratuitous-arp

arp send-gratuitous-arp命令用来在接口上使能定时发送免费ARP功能，并设置发送免费ARP报文的周期。

undo arp send-gratuitous-arp命令用来关闭定时发送免费ARP功能。

【命令】

arp send-gratuitous-arp [**interval** *milliseconds*]

undo arp send-gratuitous-arp

【缺省情况】

定时发送免费ARP功能处于关闭状态。

【视图】

三层以太网接口视图/VLAN接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin
mdc-admin

【参数】

interval *milliseconds*：发送免费ARP报文的周期，取值范围为200～200000，单位为毫秒，缺省值为2000毫秒。

【使用指导】

配置本命令后，只有当接口链路up并且配置IP地址后，此功能才真正生效。

只能为VRRP虚拟IP地址、接口主IP地址和手工配置的从IP地址发送免费ARP。主IP地址可以是手工配置或者通过其他方式获取的，但是从IP地址必须是手工配置的。

如果修改了免费ARP报文的发送周期，则在下一个发送周期才能生效。

如果同时在很多接口下使能本功能，或者每个接口有大量的从IP地址，或者两种情况共存的同时又配置很小的发送时间间隔，那么免费ARP报文的发送频率可能会远远低于用户的预期。

【举例】

#在接口Vlan-interface2上使能定时发送免费ARP功能，发送免费ARP报文的周期为300毫秒。

<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp send-gratuitous-arp interval 300