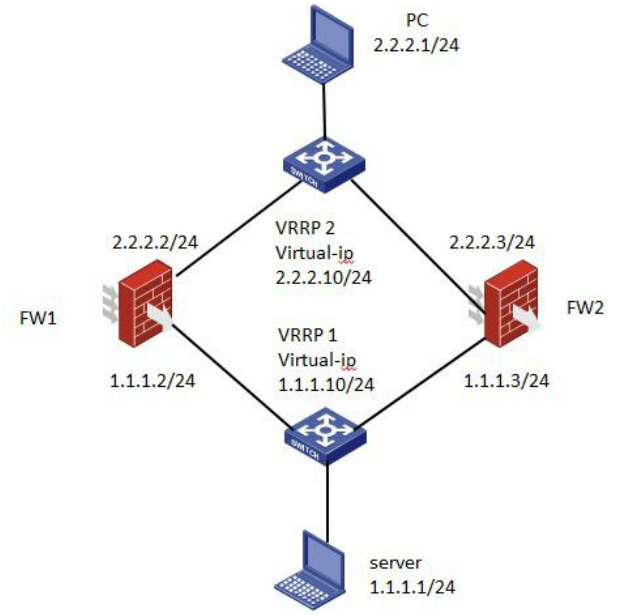
V5版本防火墙 F1000-E-SI nat联动vrrp track的经验案例分析

李聪 2016-04-12 发表



一、 组网以及问题现象：

如图组网所示，两台型号为F1000-E-SI 的FW1和FW2上面分别配置两个vrrp组。Vrrp 1的虚拟地址为1.1.1.10/24，vrrp 2的虚拟地址为2.2.2.10/24。FW1为vrrp 1组的master，同时也为vrrp 2组的master设备，并且保证vrrp 1与vrrp 2是同步切换的。现在在FW1上面和FW2上面同时配置nat server，将PC访问2.2.2.110转换为访问内网服务器。现在问题是配置了nat server以及开放策略之后，pc访问不了服务器。

二、 实验验证以及原因分析：

下面通过检查配置和实验验证的方式进行分析与论证。

1. 检查现场的防火墙的配置

FW1的配置：

在2.2.2.2/24的接口上配置：

nat server protocol icmp global 2.2.2.110 inside 1.1.1.1 track vrrp 1

FW2的配置：

在2.2.2.3/24的接口上配置：

nat server protocol icmp global 2.2.2.110 inside 1.1.1.1 track vrrp 1

从以上的配置，我们发现和路由器配置不同的地方在于配置了vrrp的时候引用了track vrrp这个参数。但是我们发现一个问题就是引用的vrrp组是1组，并不是接口所在的vrrp 2组。于是让现场修改为vrrp 2组之后能够正常访问。现在有一个问题就是为什么vrrp 1组与2组都是同步切换的，按理track动作也应该一致的，但是为什么必须track接口所在的vrrp组才行呢？下面通过实验验证一下。

2. track为接口所在vrrp组时候的分析

这时候的配置为：

nat server protocol icmp global 2.2.2.110 inside 1.1.1.1 track vrrp 2

2.1 查看master FW1上面的路由信息

2.2.2.110/32 Static 1 0 0.0.0.0 NULL0

查看slave FW2上面的路由发现没有产生null 0的路由信息。平时我们也可以发现，不管防火墙还是路由器，配置了nat之后都会产生null 0的路由。原因是NAT使用的公网地址，包括了被引用的地址池的地址、NAT Server的公网地址和被引用的静态配置的公网地址。这些地址全部会进入地址管理模块进行统一地址管理，并由地址管理模块通知路由管理模块将这些IP地址加入路由表。当外部设备向这些地址发起ARP请求，设备便会将ARP请求送到地址管理模块检查ARP报文的合法性，地址管理发现ARP所请求的IP地址为NAT地址池地址，则通知NAT模块判断是否需要回应ARP，NAT模块会检查ARP所请求的IP地址是否是收到ARP接口下配置的NAT的地址，如果是则通知ARP模块进行ARP应答。由于有了地址统一管理，与接口不在同一网段的地址池的地址被加入本地路由表，并且可以有选择的将其引入动态路由协议，通过OSPF或者BGP将其发布出去，简化了组网中其他设备的配置。

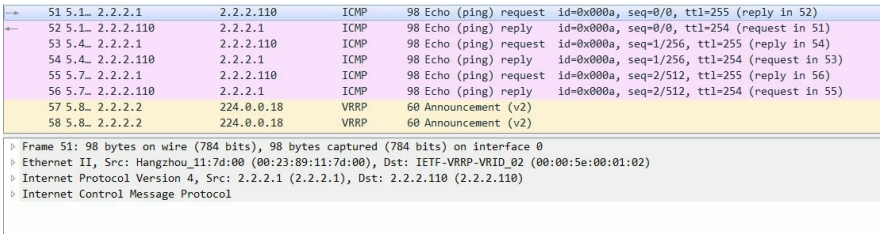
2.2 在master查看虚拟mac地址

通过在防火墙上面执行dis vrrp ver查看vrrp的状态以及虚拟mac地址：

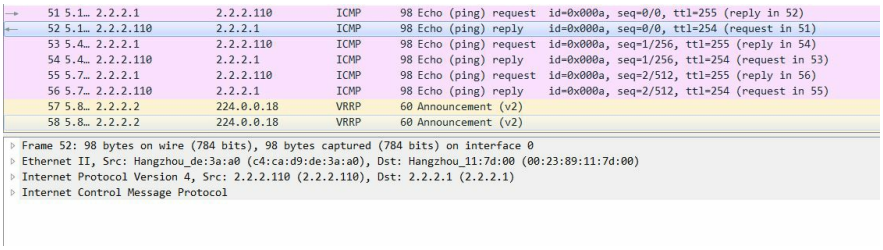
```
[F1000-E-SI]dis vrrp ver
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 2
   Interface GigabitEthernet0/1
     VRID           : 1              Adver Timer : 1
     Admin Status   : Up             State       : Master
     Config Pri     : 150            Running Pri : 150
     Preempt Mode   : Yes            Delay Time  : 0
     Auth Type      : None
     Virtual IP     : 1.1.1.10
     Virtual MAC    : 0000-5e00-0101 //vrrp 1的虚拟mac地址
     Master IP      : 1.1.1.2

   Interface GigabitEthernet0/2
     VRID           : 2              Adver Timer : 1
     Admin Status   : Up             State       : Master
     Config Pri     : 150            Running Pri : 150
     Preempt Mode   : Yes            Delay Time  : 0
     Auth Type      : None
     Virtual IP     : 2.2.2.10
     Virtual MAC    : 0000-5e00-0102 //vrrp 2的虚拟mac地址
     Master IP      : 2.2.2.2
```

2.3 在pc上面wireshark抓包结果：

请求报文：



回应报文：



从以上抓包发现pc请求2.2.2.110的时候，对应请求的mac地址就是虚拟mac地址。而回应的时候就是master设备的接口mac地址回应报文的请求。

3. track为其他vrrp组时候的分析

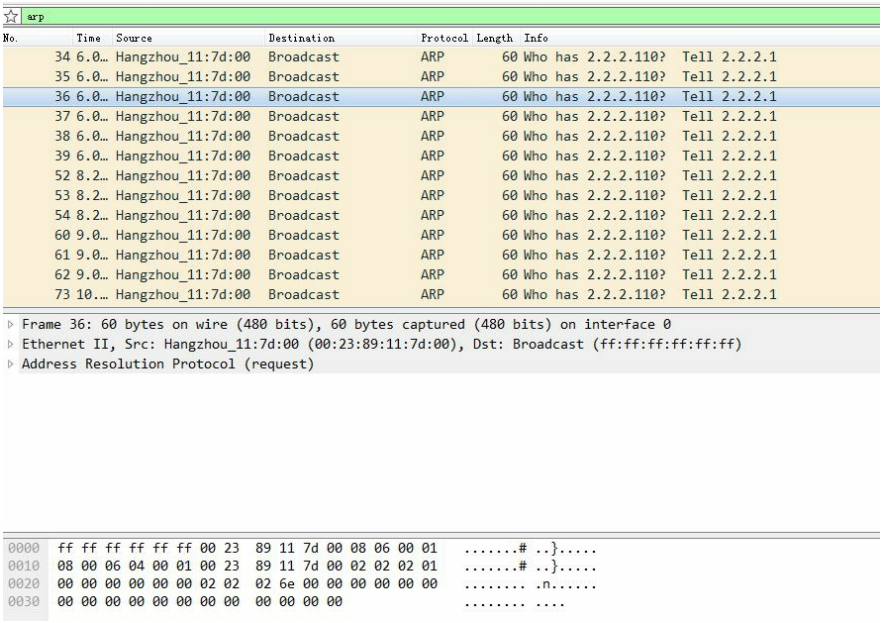
这时候的配置为：

nat server protocol icmp global 2.2.2.110 inside 1.1.1.1 track vrrp 1

3.1 查看master FW1上面的路由信息

通过查看master FW1上面的路由信息发现没有产生null 0的路由，slave设备上面也没有产生null 0的路由。由此可见设备没有产生路由，不会对外网访问nat server地址池的请求作出arp回应。

3.2 查看pc上面的抓包信息



我们发现pc发送的请求没有得到任何的回应，当然nat server不会生效。

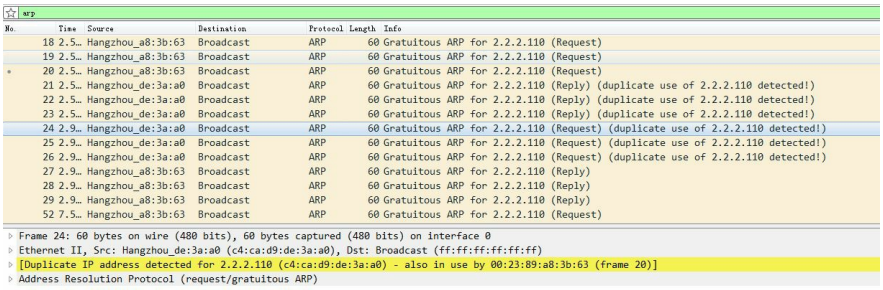
4. nat server不引用任何vrrp组时候的分析

如果不引用track vrrp的时候nat server又是不通的，下面将配置中的track vrrp去掉之后进行分析。

4.1 查看master FW1以及slave FW2上面的路由信息

去掉配置中的track之后发现两个FW上面都会产生null 0的路由，同时两台设备报地址冲突的提示，提示冲突的mac地址就是分别是另外一台的接口的mac地址信息。

4.2 查看pc上面的抓包信息



从以上的信息看出，pc抓包也提示同一个地址2.2.2.110被两个mac地址使用，这两个地址就是主设备的接口mac地址以及备设备的接口mac地址。

5. nat server与track关联的总结

如果没有配置地址池和nat server的vrrp参数，arp请求或应答中携带的MAC地址是该网口的MAC，如果配置了vrrp参数，发送的arp就是VRRP虚拟MAC地址。如果不配置VRRP的话，还会带来一个问题就是防火墙在收到对nat地址的ARP请求的时候无法判断是否需要回应ARP响应（特别是在互为备份的组网中），如果主备都回应arp响应的话首先不能保证arp响应的mac地址的正确性，其次不能保证与防火墙相连的三层交换机上的arp地址转发表的正确性，所以在双机热备的组网中nat的配置一定要在后面加上vrrp id，对于nat server的配置也是如此。

三、 解决办法：

1. 接口下配置nat server的track vrrp组，所引用的组必须是nat server接口所在的vrrp组。

2. 引用的track vrrp组不能引用其他vrrp组或者不配置。