



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:

51	5.1..	2.2.2.1	2.2.2.110	ICMP	98 Echo (ping) request	id=0x000a, seq=0/0, ttl=255 (reply in 52)
52	5.1..	2.2.2.110	2.2.2.1	ICMP	98 Echo (ping) reply	id=0x000a, seq=0/0, ttl=254 (request in 51)
53	5.4..	2.2.2.1	2.2.2.110	ICMP	98 Echo (ping) request	id=0x000a, seq=1/256, ttl=255 (reply in 54)
54	5.4..	2.2.2.110	2.2.2.1	ICMP	98 Echo (ping) reply	id=0x000a, seq=1/256, ttl=254 (request in 53)
55	5.7..	2.2.2.1	2.2.2.110	ICMP	98 Echo (ping) request	id=0x000a, seq=2/512, ttl=255 (reply in 56)
56	5.7..	2.2.2.110	2.2.2.1	ICMP	98 Echo (ping) reply	id=0x000a, seq=2/512, ttl=254 (request in 55)
57	5.8..	2.2.2.2	224.0.0.18	VRRP	60 Announcement (v2)	
58	5.8..	2.2.2.2	224.0.0.18	VRRP	60 Announcement (v2)	

Frame 51: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: Hangzhou_11:7d:00 (00:23:89:11:7d:00), Dst: IETF-VRRP-VRID_02 (00:00:5e:00:01:02)
Internet Protocol Version 4, Src: 2.2.2.1 (2.2.2.1), Dst: 2.2.2.110 (2.2.2.110)
Internet Control Message Protocol

回应报文:

51	5.1..	2.2.2.1	2.2.2.110	ICMP	98 Echo (ping) request	id=0x000a, seq=0/0, ttl=255 (reply in 52)
52	5.1..	2.2.2.110	2.2.2.1	ICMP	98 Echo (ping) reply	id=0x000a, seq=0/0, ttl=254 (request in 51)
53	5.4..	2.2.2.1	2.2.2.110	ICMP	98 Echo (ping) request	id=0x000a, seq=1/256, ttl=255 (reply in 54)
54	5.4..	2.2.2.110	2.2.2.1	ICMP	98 Echo (ping) reply	id=0x000a, seq=1/256, ttl=254 (request in 53)
55	5.7..	2.2.2.1	2.2.2.110	ICMP	98 Echo (ping) request	id=0x000a, seq=2/512, ttl=255 (reply in 56)
56	5.7..	2.2.2.110	2.2.2.1	ICMP	98 Echo (ping) reply	id=0x000a, seq=2/512, ttl=254 (request in 55)
57	5.8..	2.2.2.2	224.0.0.18	VRRP	60 Announcement (v2)	
58	5.8..	2.2.2.2	224.0.0.18	VRRP	60 Announcement (v2)	

Frame 52: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: Hangzhou_de:3a:a0 (c4:ca:d9:de:3a:a0), Dst: Hangzhou_11:7d:00 (00:23:89:11:7d:00)
Internet Protocol Version 4, Src: 2.2.2.110 (2.2.2.110), Dst: 2.2.2.1 (2.2.2.1)
Internet Control Message Protocol

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

No.	Time	Source	Destination	Protocol	Length	Info
34	6.0...	Hangzhou_11:7d:00	Broadcast	ARP	60	Who has 2.2.2.110? Tell 2.2.2.1
35	6.0...	Hangzhou_11:7d:00	Broadcast	ARP	60	Who has 2.2.2.110? Tell 2.2.2.1
36	6.0...	Hangzhou_11:7d:00	Broadcast	ARP	60	Who has 2.2.2.110? Tell 2.2.2.1
37	6.0...	Hangzhou_11:7d:00	Broadcast	ARP	60	Who has 2.2.2.110? Tell 2.2.2.1
38	6.0...	Hangzhou_11:7d:00	Broadcast	ARP	60	Who has 2.2.2.110? Tell 2.2.2.1
39	6.0...	Hangzhou_11:7d:00	Broadcast	ARP	60	Who has 2.2.2.110? Tell 2.2.2.1
52	8.2...	Hangzhou_11:7d:00	Broadcast	ARP	60	Who has 2.2.2.110? Tell 2.2.2.1
53	8.2...	Hangzhou_11:7d:00	Broadcast	ARP	60	Who has 2.2.2.110? Tell 2.2.2.1
54	8.2...	Hangzhou_11:7d:00	Broadcast	ARP	60	Who has 2.2.2.110? Tell 2.2.2.1
60	9.0...	Hangzhou_11:7d:00	Broadcast	ARP	60	Who has 2.2.2.110? Tell 2.2.2.1
61	9.0...	Hangzhou_11:7d:00	Broadcast	ARP	60	Who has 2.2.2.110? Tell 2.2.2.1
62	9.0...	Hangzhou_11:7d:00	Broadcast	ARP	60	Who has 2.2.2.110? Tell 2.2.2.1
73	10...	Hangzhou_11:7d:00	Broadcast	ARP	60	Who has 2.2.2.110? Tell 2.2.2.1

▶ Frame 36: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 ▶ Ethernet II, Src: Hangzhou_11:7d:00 (00:23:89:11:7d:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 ▶ Address Resolution Protocol (request)

0000	ff ff ff ff ff ff 00 23	89 11 7d 00 08 06 00 01# ..}.....
0010	08 00 06 04 00 01 00 23	89 11 7d 00 02 02 02 01# ..}.....
0020	00 00 00 00 00 00 02 02	02 6e 00 00 00 00 00 00n.....
0030	00 00 00 00 00 00 00 00	00 00 00 00

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

No.	Time	Source	Destination	Protocol	Length	Info
18	2.5...	Hangzhou_a8:3b:63	Broadcast	ARP	60	Gratuitous ARP for 2.2.2.110 (Request)
19	2.5...	Hangzhou_a8:3b:63	Broadcast	ARP	60	Gratuitous ARP for 2.2.2.110 (Request)
20	2.5...	Hangzhou_a8:3b:63	Broadcast	ARP	60	Gratuitous ARP for 2.2.2.110 (Request)
21	2.5...	Hangzhou_de:3a:a0	Broadcast	ARP	60	Gratuitous ARP for 2.2.2.110 (Reply) (duplicate use of 2.2.2.110 detected!)
22	2.5...	Hangzhou_de:3a:a0	Broadcast	ARP	60	Gratuitous ARP for 2.2.2.110 (Reply) (duplicate use of 2.2.2.110 detected!)
23	2.5...	Hangzhou_de:3a:a0	Broadcast	ARP	60	Gratuitous ARP for 2.2.2.110 (Reply) (duplicate use of 2.2.2.110 detected!)
24	2.9...	Hangzhou_de:3a:a0	Broadcast	ARP	60	Gratuitous ARP for 2.2.2.110 (Request) (duplicate use of 2.2.2.110 detected!)
25	2.9...	Hangzhou_de:3a:a0	Broadcast	ARP	60	Gratuitous ARP for 2.2.2.110 (Request) (duplicate use of 2.2.2.110 detected!)
26	2.9...	Hangzhou_de:3a:a0	Broadcast	ARP	60	Gratuitous ARP for 2.2.2.110 (Request) (duplicate use of 2.2.2.110 detected!)
27	2.9...	Hangzhou_a8:3b:63	Broadcast	ARP	60	Gratuitous ARP for 2.2.2.110 (Reply)
28	2.9...	Hangzhou_a8:3b:63	Broadcast	ARP	60	Gratuitous ARP for 2.2.2.110 (Reply)
29	2.9...	Hangzhou_a8:3b:63	Broadcast	ARP	60	Gratuitous ARP for 2.2.2.110 (Reply)
52	7.5...	Hangzhou_a8:3b:63	Broadcast	ARP	60	Gratuitous ARP for 2.2.2.110 (Request)

▶ Frame 24: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 ▶ Ethernet II, Src: Hangzhou_de:3a:a0 (c4:ca:d9:de:3a:a0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 ▶ [Duplicate IP address detected for 2.2.2.110 (c4:ca:d9:de:3a:a0) - also in use by 00:23:89:a8:3b:63 (frame 20)]
 ▶ Address Resolution Protocol (request/gratuitous ARP)

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。