MSR堆叠设备跨框NAT映射不生效

NAT IRF 罗梦恺 2022-01-10 发表

组网及说明

内网服务器----MSR56（IRF）----外网终端

问题描述

两台MSR5660做了IRF堆叠作为某局点的出口设备，外网接口为G1/2/0/0和G2/2/0/0，在接口下配置了NAT server，内网接口为静态聚合口，该聚合口对接内网防火墙，由于防火墙接口做的是冗余，所以路由器静态聚合口接口下配置了link-aggregation selected-port maxumum 1 ，选中的是1 框的口，在聚合接口下配置了service chassis 1 slot 2。路由上的缺省路由走的是G1/2/0/0，全局下配置了session synchronization enable保持会话同步，同时在G1/2/0/0和G2/2/0/0下配置了ip last-hop hold保持报文交互来回路径一致。**现场只有一框的G1/2/0/0接口能成功映射但是二框的G2/2/0/0无法映射。**

现场配置如下：

```
#
interface GigabitEthernet1/2/0/0
 port link-mode route description CUCC
 bandwidth 200000
 combo enable copper
 ip address 221.7.XXX.XXX 255.255.255.240
 ip last-hop hold
 nat outbound 3000
nat server protocol tcp global current-interface 20211 inside 10.13.XXX.XXX 20211
#
 interface GigabitEthernet2/2/0/0
 port link-mode route description CMCC
 bandwidth 200000
 combo enable copper
 ip address 36.136.XXX.XXX 255.255.255.192
 ip last-hop hold
 nat outbound 3000
 nat server protocol tcp global current-interface 20211 inside 10.13.XXX.XXX 20211
#
interface Route-Aggregation4
 description TO-F1000
 service chassis 1 slot 2
 service standby chassis 2 slot 2
 ip address 10.13.XXX.XXX 255.255.255.252
 ospf network-type p2p
 link-aggregation selected-port maximum 1
 tcp mss 1280
 qos apply policy ADWAN-QPInRAGG4 inbound
 nat hairpin enable
#
session synchronization enable
 session synchronization dns http
```

过程分析

现场二框在映射的时候发现NAT设备上是存在相应的nat会话的，这说明入方向的映射过程没问题，但是后续的回程报文可能在某个环节丢弃了。通过debug ip packet 可以看到报文交互的过程。看到报文在回到内网聚合口的时候因为FIB BLACKHOLE丢弃了。推测是由于内网聚合口只选中了1框，所以二框的映射报文前往内网服务器需要走一框，同时回程报文也是回到1框，因为缺省路由走的一框，从一框出口出去但是没找到会话，所以报文丢弃。在上述组网和配置下可能IRF会话同步和ip last-hop hold未生效。

*Dec 31 15:27:32:408 2021 NNYY_04FDCRT03101 IPFW/7/IPFW_PACKET: -Chassis=1-Slot=2;
Discarding, interface = ifIndex:10881
version = 4, headlen = 20, tos = 0
pktlen = 52, pktid = 54339, offset = 0, ttl = 251, protocol = 6
checksum = 6939, s = 10.13.XXX.XXX, d = 183.242.XXX.XXX
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Special outgoing interface FIB BLACKHOLE.
Payload: TCP
source port = 20211, destination port = 14662
sequence num = 0x3029b259, acknowledgement num = 0x67ee4ec3, flags = 0x12
window size = 65535, checksum = 0x7e39, header length = 32.

解决方法

上述案例中的问题：

1、外网接口是以太口，并非全局口，这种情况下会话同步功能不生效。可以将设备外网接口的配置移到聚合口下，如: 新建两个聚合口，现场的2/2/0/0 放在聚合口A，1/2/0/0放在聚合口B ，将以太口下的配置复制到相应聚合口下。

2、Ip last-hop hold enable针对于同框非跨板转发场景，对于跨框需求还需要在全局下配置 ip last-hop backup enable

3、缺少会话热备配置

堆叠设备跨框的NAT映射或者hairpin的处理方法：

1、外网全局聚合接口，内网全局聚合接口，聚合接口不需要配置service slot。

2、同时配置会话同步保证会话自动在两个框之间同步。（该命令只能同步全局接口的会话，所以要配置全局口）

Session synchronization enable （R0809P25以后版本）

3、对于MSR5660设备要进行热备配置

failover group 1

bind chassis 1 slot 2 primary

bind chassis 2 slot 2 secondary

4、在接口下配置ip last-hop hold，在全局下配置 **last-hop backup enable。**