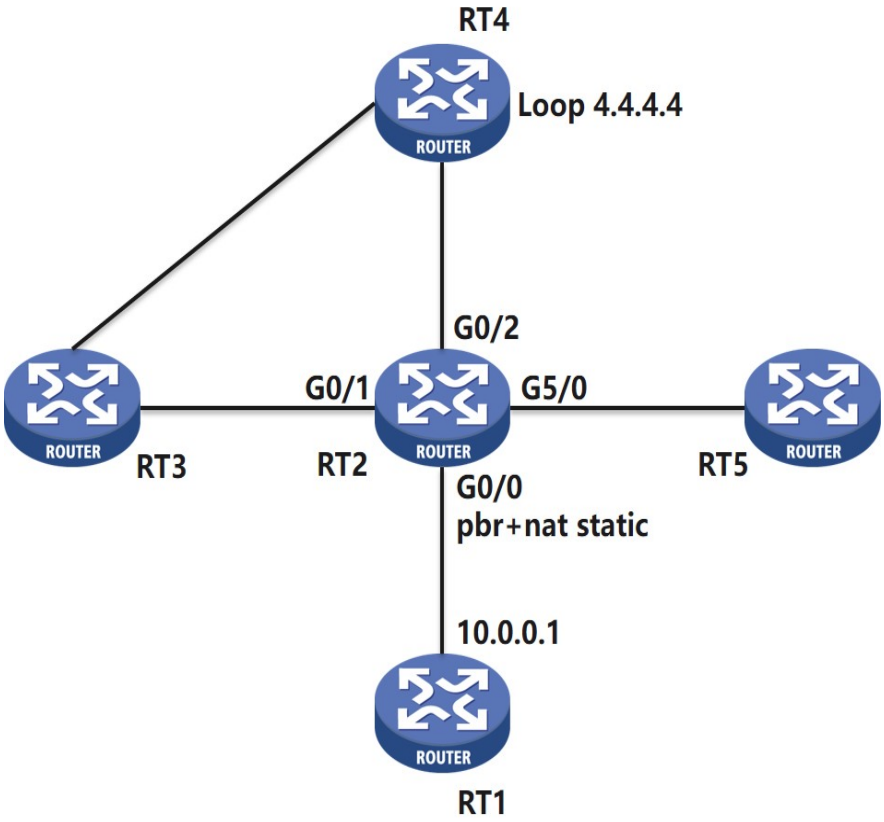
SR6616策略路由+单臂+nat组网不通问题经验案例

策略路由 郭昊 2019-10-22 发表

组网及说明



组网中RT2做pbr和nat，对RT1访问2.2.2.2的流量做nat转换目的地址为4.4.4.4，并将该流量通过pbr扔到右侧流量清洗设备RT5，从RT5回来后扔给RT4。

问题描述

现场做配置后10.0.0.1 ping 2.2.2.2不通。RT2对于回程流量没有做nat。

过程分析

先考虑PBR，此类PBR+单臂的组网，RT2需要开undo ip fast-forwarding load-sharing，将流量入接口作为快转的一个标志，避免流量从G0/0和G5/0到RT2时都匹配到同一条快转导致环路。详细内容可以参考案例https://zhiliao.h3c.com/Theme/details/5620。

再考虑nat问题。检查现场设备配置，全局nat static outbound 4.4.4.4 2.2.2.2，接口G0/0下nat static enable，没问题。接下来需要看流量停在哪一步。

首先RT2上面debug nat packet，发现有10.0.0.1 ping 2.2.2.2的流量转换为了10.0.0.1 ping 4.4.4.4，出方向nat没问题。之后对10.0.0.1 ping 4.4.4.4的流量做流统，G5/0有发有收，说明PBR和流量清洗设备都没问题；G0/2出方向有包，入方向没包，说明回程报文异常，至少流量没有从出接口回来；由于排查过程中无法操作RT4，因此只能在RT2其他所有接口入方向流统，看报文是否从其他接口回来，发现回程流量入接口为G0/1，推测RT4回程路由指向RT3。流量回到了RT2，但是没有转给RT1，加上debug的现象，说明回程流量没有做nat。

结合上面PBR的情况容易联想到，由于开了undo ip fast-forwarding load-sharing，所有流量从G0/1进到RT2时，匹配不到已有快转表。而nat会话是跟快转表关联的，所以回程流量没有做nat。要解决这个问题，需要流量从原接口回来，来回路径一致即可。

解决方法

1. 调整RT4路由，使来回路径一致；
2. RT2流量出口G0/2做nat outbound，改变报文源地址，这样RT4回程报文目的地址为RT2接口G0/2地址，肯定会发到G0/2；
3. RT2接口G0/1再做一个pbr，将流量扔到清洗设备再绕一圈，流量回到G5/0时能匹配到快转和nat会话；
4. 在RT2和RT3的上行口G0/2都做nat inbound static转目的地址，不在下行口G0/0做nat outbound static，即使回程流量回到RT3，也可以由RT3做nat。