某局点LB链路切换后部分流量不通

outbound链路负载均衡 陈阳 2023-12-25 发表

组网及说明

LB作为分流设备，有A、B两条上行链路，每条链路上行都是一台防火墙设备，然后专线到总部路由器，A作为主链路，业务默认走A，当A链路出现异常时切换到B链路，A链路恢复后再切换到A链路。

问题描述

现场模拟A链路故障，在LB上将A口shutdown，此时流量正常切换到B链路，业务访问正常，将A口undo shutdown后，业务不通。

过程分析

经过测试，确认信息如下：

1、A和B链路均正常的情况下，业务流量走A链路，当A链路故障后，流量切换到备用链路B，此时流量不会中断；

2、将A链路恢复，由于此时LB的B链路是正常的，会话不会老化，流量仍然按照会话进行转发到B链路上，通过抓包发现对端路由器将流量从A链路发回来，此时由于来回路径不一致（去的流量走B，回来的流量走A）导致报文被ASPF丢弃；

*Nov X 15:06:33:360 202X H3C SecPath F1000_X.X.X.X ASPF/7/PACKET: -COntext=1; The first packet was dropped by ASPF for invalid status. Src-ZOne=Untrust, Dst-ZOne=Trust;If-In=GigabitEthernet1/0/X, If-Out=GigabitEthernet1/0/X, VLAN-In=X, VLAN-Out=X; Packet Info:Src-IP=X.X.X.X, Dst-IP=X.X.X.X, VPN-Instance=none, Src-Port=1, Dst-Port=0. Protocol=ICMP(1).

3、A链路恢复后，通过手动删除会话reset session all，流量可以立即恢复连通；

4、综上所述，确认链路恢复后流量不通的原因是本端LB按照会话转发流量到B链路，而对端路由器检测到A链路恢复，将流量从A链路发回，导致来回路径不一致。

解决方法

通过在LB配置EAA脚本，track A链路状态，当A链路恢复时，立即触发会话清除命令，让会话重新建立，转发到A链路上即可。