

知 ACG1000没有绑定MAC的用户10秒之内可以上网

域间策略/安全域

赛祖尧

2019-08-26 发表

组网及说明

现场ACG位于核心交换机上行，下面所有用户的网关都在核心交换机上

问题描述

现场配置为只有绑定了MAC地址的用户可以上网，但是用户发现有一些没有绑定MAC地址的用户刚刚接入网络的前10秒是可以正常上网的，10秒种之后策略才生效，该用户被限制上网

过程分析

现场最开始怀疑是ACG的识别机制，导致可以方通最开始用户上网的几个报文用来识别MAC地址，但是客户现场的现象是没有绑定MAC地址的终端刚刚接入网络中的10秒钟之内是可以上网的。
用户为了实现需求，实际上是在ACG上开启了跨三层MAC地址学习功能。
后续抓包发现，在绑定MAC地址的终端接入网络的前10秒钟，终端上网其实是携带了核心交换机的MAC地址进行上网，但是按照正常的配置来说这个携带了核心交换机的MAC应该也是不能上网的。
后续分析现场的用户配置之后发现，现场有一个用户绑定的MAC地址为核心交换机的MAC地址，这就导致了没有绑定MAC地址的终端刚刚接入网络中的10秒钟之内是使用核心交换机的MAC地址进行上网的，后续跨三层MAC地址学习生效之后，设备识别为终端真实的MAC地址，这个时候由于没有进行绑定，所以被拒绝上网。

解决方法

修改ACG侧配置，修改绑定了核心交换机互联ACG的接口的MAC地址的用户，把其绑定的MAC地址修改为真实的MAC地址