SecPath ACG1000-BE DHCP分配地址异常的解决办法

DHCP　高子军　2019-09-28 发表

组网及说明

无

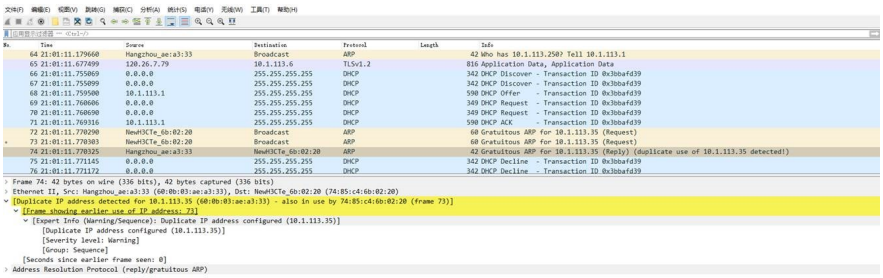
问题描述

ACG1000作为公网出口设备，内网用户的网关，在设备上配置了DHCP服务器。设备一直运行正常，近期突然出现无线终端无法上网的情况，排查发现是因为终端无法获取到IP地址导致的。

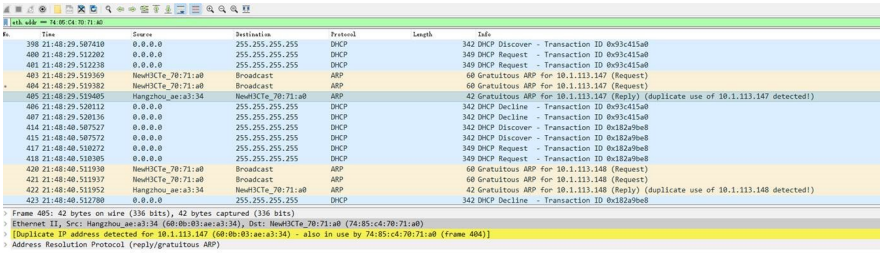
过程分析

1.经过查看设备信息，做如下的测试：

测试一：设备2口连接外网，只保留了设备的2口、5口、8口测试，其他接口都DOWN掉。5口连接一台PC，能正常获取到IP地址，8口下联了二层交换机，交换机下联AP法获取到IP地址。通过在8口抓包发现，AP在获取到IP地址后，发送免费ARP报文，设备回应了报文提示IP地址已被占用，所以AP重新去获取IP地址，一直获取不到。设备回应的报文内，MAC地址是设备3口的MAC地址，但是3口是down的状态。



测试二：只保留设备的2口、5口、7口；其中7口是直连AP，中间没有二层交换机。同时将GE3从网桥接口（BVI）内排除出去。此时在设备的GE7抓包和第一次测试时是一样的现象，但是回包内的MAC地址变为了GE4口的MAC地址，GE4口也是down的。



2.从两次测试的抓包来看，确实是设备侧的问题。进一步排查现场的配置，发现有如下的异常配置，将配置删除后解决。

	ID	源地址	目的地址	服务	接口	转换后目的地址	转换后端口	日志	操作
1	1	any	外网	8001	ge2	服务器	8001	-	
2	2	any	外网	8002	ge2	服务器	8002	-	
3	3	any	外网	3306	ge2	服务器	3306	-	
4	4	any	外网	6379	ge2	服务器	6379	-	
5	5	any	any	8001	bvi1	服务器	8001	-	
6	6	any	any	8002	bvi1	服务器	8002	-	
7	7	any	any	3306	bvi1	服务器	3306	-	
8	8	any	any	6379	bvi1	服务器	6379	-	

解决方法

当ACG配置DNAT时设备会检测策略中配置的目的地址，当收到关于目的地址的ARP请求时就会回应该地址在ACG设备上。

该机制为了当ACG出口的地址为一个大网段时，也可以做相应的目的地址映射。