某局点部分手机连上无线以后出现前一分钟无法上网的情况

攻击检测及防范　阮威　2020-02-28 发表

组网及说明

AC旁挂核心，集中转发，无线业务网关在核心交换机上，portal认证

问题描述

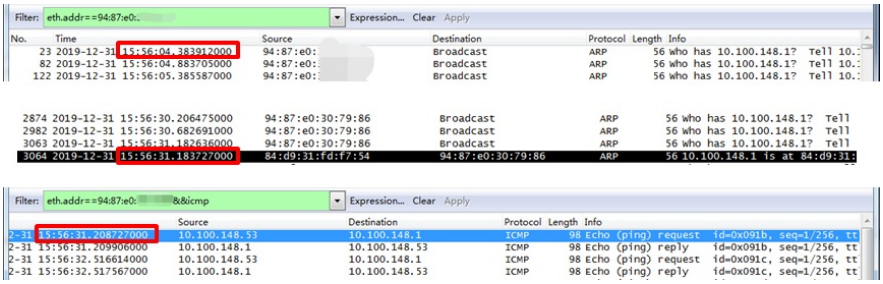
部分手机连上无线以后出现前一分钟左右无法上网的情况，一分钟以后故障消除

过程分析

1.通过display wlan client 发现终端上线过程没有问题，拿地址正常，但是从网关ping终端发现前一分钟左右不通，在不通时网关和终端都没有互相学习到对方的ARP。

2.为确定是否与AC转发以及认证有关，创建一个空服务模板并选定转发方式为本地转发，发现故障现象依旧，说明与AC和认证没有关系。

3.在AP上行口抓包，抓包的同时终端一直ping网关，可以看到终端从15:56:04时开始发送ARP请求来请求网关的ARP，但是网关直到15:56:31时才回复第一个ARP请求，回复ARP报文后几乎同一时间PING包就通了，说明问题出在了ARP的学习上，PING过程并未有延迟。



4.那么网关为何会延迟这么久才回复ARP请求呢？查看网关侧配置，发现其配置了ARP防攻击检测：

arp source-mac filter

在5秒内收到同一源MAC地址发送的ARP超过一定阈值（缺省30个）则将此MAC地址添加到攻击检测表项中

arp source-mac aging-time 60

修改ARP攻击检测表项的老化时间为60秒，缺省为300秒

5.当该类终端接入无线时会在短时间内发出大量ARP请求从而触发ARP防攻击检测机制，导致该MAC被加入到攻击检测表项中，当表项老化时间60秒过去后，网关才回复终端的ARP请求

解决方法

去掉ARP防攻击检测或将ARP防攻击检测的阈值调高，例如：arp source-mac threshold 100，表示在5秒内收到同一源MAC地址发送的ARP超过100（缺省30）个才将此MAC地址添加到攻击检测表项中