某局点终端频繁切换SSID导致portal概率性无感知不成功

Portal 孙建刚 2021-12-13 发表

组网及说明

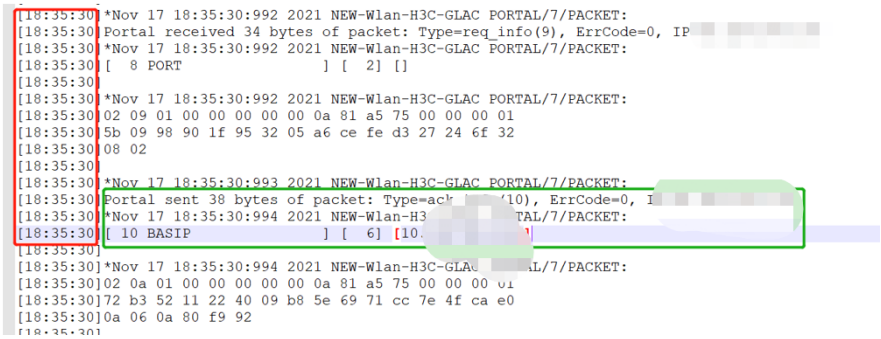
AC旁挂核心，集中转发常规组网

问题描述

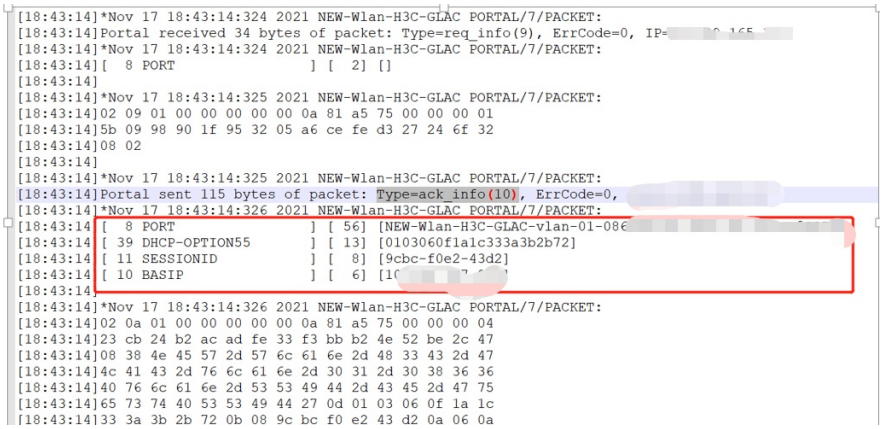
正常情况下终端链接portal无感知的SSID认证正常，频繁的同另一SSID来回切换时， 个别终端小概率性会出现“向 Portal Server 发送请求超时”的报错 。

过程分析

复现时查看服务器与设备上的debug日志，服务器上在收到设备发送的ack_info后查询设备信息不合法，便继续向设备发送req_info请求。此时查看设备上的信息发现设备在处理ack_info时，出现ip反查client信息异常问题，由于IP反查client失败，导致无法携带服务器要求的信息，进而后续无法认证，如下绿框为回复的ack_info携带信息异常，可以看到此portal过程发生在18:35:30时间



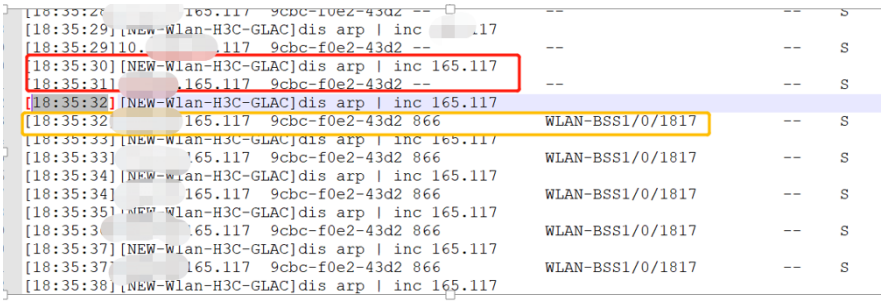
而正常认证时设备通过终端触发portal携带的ip信息是能够反查到设备信息的，并做填充相关属性携带到ack_info报文中供服务器查询，如下是该终端正常认证时的设备回复ack_info时的封装信息：



结合分析过程：在出现问题时，设备回复的ack_info信息填充错误，进而导致认证过程失败，引起反查失败的可能原因：

portal反查IP，是根据IP地址反查是哪个client，然后获取相关信息。client学习IP地址有两种方式，设备截获client的DHCP和截获client的ARP。两种方式没有优先级，后面学习到的会覆盖前面学习到的。

目前出现该问题的原因为终端在链接到portal无感知SSID时，终端获取ip地址后，未能向其他正常终端发送免费ARP更新表项，便发起ip数据包触发portal认证流程，上图18:35:30时该终端的portal认证流程已经到了ack_info阶段，而我们在对该终端配置静态ARP的情况下，直到18:35:32才看到该终端上报免费ARP，设备学到该终端ARP并更新到wlan snooping表项中，比该终端触发portal流程晚了2秒：



所以，由于终端未按照正常流程优先发送免费ARP便发送ip数据包的行为导致设备正常做ip反查client时无相关信息查询，进而回复IMC服务器的ack_info信息不能携带有效信息。

解决方法

Portal认证协议机制是以终端的ip触发的，若终端获取ip后未能及时发送免费ARP更新表项，存在短暂设备对该终端信息无法及时学习，应对这种特殊场景下的终端行为，我们可在集中转发模式下开启无线Portal客户端合法性检查功能：

[AC] portal host-check enable

缺省情况下，设备仅根据ARP表项对无线Portal客户端进行合法性检查。本功能开启后，当设备收到未认证Portal用户的认证报文后，将使用WLAN Snooping表、DHCP Snooping表和ARP表对其进行合法性检查。如果在这三个表中查询到该Portal客户端信息，则认为其合法并允许进行Portal认证。