V7 portal结合ldap认证失败问题

Portal 陆启隆 2021-09-27 发表

组网及说明

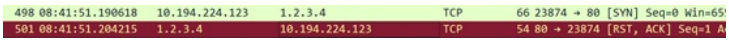
普通无线组网，使用v7 ac，终端的网关和dhcp server在核心交换机。

问题描述

终端可以接入无线服务，并获取到地址，部分终端可以重定向完成portal认证，部分终端无法重定向，在浏览器中手动输入ip地址依旧无法重定向。

过程分析

部分终端可以portal认证通过，而部分终端无法通过，并无法重定向，应关注故障终端的认证过程。
现场在核心连接ac的接口上镜像抓包发现。



终端在浏览器中输入1.2.3.4，发现并没有对应的http报文。进一步检索发现tcp连接就没有建立起来，终端发送第一个syn报文后，ac直接回复reset报文。
Ac直接回复reset报文是tcp异常终止，该现象很不常见，由于该终端连接其他不认证ssid可以正常上网，终端的tcp报文发送应该不会存在问题。Ac可以给其他部分终端重定向，所以ac的tcp功能也应是没问题的。所以需要考虑ac为何认为终端发送的报文异常，优先考虑表象是否异常。
Debug信息中的报错
*Sep 9 16:28:50:612 2021 AC PORTAL/7/MAC-
trigger Error: The user (IP=10.194.224.19) already exists, user MAC=4c02-2076-e60f, Ignored the new MAC event.
查看ac上终端的client表象为，ip1,mac1，但是查看portal表象为ip1,mac2.由此可知是由于表象冲突导致终端无法触发重定向。
Portal表象
Username: 4C:02:20:76:E6:0F
AP name: ap1
Radio ID: 2
SSID: test
Portal server: test
State: Online
VPN instance: N/A

MAC	IP	VLAN	Interface
4c02-2076-e60f	10.194.224.19	224	WLAN-BSS2/0/8824

故障终端信息

进一步排查Portal表象为何会冲突，查看现场的dhcp server发现地址池并不充裕，且ac上没有配置authorization-attribute idle-cut。导致portal终端表象会一直残留。

解决方法

扩充dhcp server，同时配置authorization-attribute idle-cut后故障解除。