某局点WX5510E与第三方服务器结合做认证失败经验案例

wlan接入 802.1X AAA VLAN 樊昊 2016-02-01 发表

某客户反馈我司无线控制器WX5510E加瘦AP组网下，通过第三方服务器下发VLAN，但下发不成功，IMC可以成功下发。登录之后查看

Index=9602, Username=10000269@fordot1x
MAC=00-1B-77-08-4E-26
IP=N/A
IPv6=N/A
Access=8021X ,AuthMethod=EAP
Port Type=Wireless-802.11,Port Name=WLAN-DBSS4:6101
Initial VLAN=3800, Authorization VLAN=N/A
ACL Group=Disable
User Profile=N/A
CAR=Disable
Traffic Statistic:
InputOctets =5183 OutputOctets =13960
InputGigawords=0 OutputGigawords=0
Priority=Disable
SessionTimeout=N/A, Terminate-Action=N/A
Start=2016-01-23 16:57:04 ,Current=2016-01-23 17:26:35 ,Online=00h29m31s
Total 1 connection matched.

发现没有进入下发的授权vlan 3810。

通过一线反馈现场无线控制器配置，

radius scheme fordot1x

server-type extended

primary authentication 192.168.0.188 key cipher c3$TB29djawx9tynalUS3bEYN9QbSz4qab73LVTOA==

primary accounting 192.168.0.188 key cipher c3$rzzTWPHX85x6Kem0wd0tMjUaAtWO/8sU/IlvKg==

user-name-format without-domain

accounting-on enable

查看配置无问题，且IMC下发正常,于是搜集AC上Radius的debug信息；

*Jan 23 15:45:42:960 2016 WX5510E RDS/7/DEBUG:

[64 Tunnel-Type] [6] [13]

[65 Tunnel-Medium-Type] [6] [6]

[81 Tunnel_Private_Group_ID] [6] [33383130]

[1 User-name] [10] [21300115]

[32 NAS-Identifier] [9] [WX5510E]

[5 NAS-Port] [6] [16781359]

[87 NAS_Port_Id] [35] [slot=1;subslot=0;port=1;vlanid=47]

[61 NAS-Port-Type] [6] [19]

[31 Caller-ID] [19] [44382D42422D32432D45322D34432D4344]

[30 Called-station-Id] [28] [70-BA-EF-89-F7-20:SITC-11x]

[40 Acct-Status-Type] [6] [3]

[45 Acct-Authentic] [6] [1]

*Jan 23 15:45:42:960 2016 WX5510E RDS/7/DEBUG:

[44 Acct-Session-Id] [20] [11600231533b1aa1e0]

[8 Framed-Address] [6] [192.168.47.75]

[4 NAS-IP-Address] [6] [192.168.250.120]

[55 Event-Timestamp] [6] [1453535142]

[H3C-26 Connect_ID] [6] [5225]

[H3C-1 Input_Peak_Rate] [6] [0]

*Jan 23 15:45:42:961 2016 WX5510E RDS/7/DEBUG:

[H3C-2 Input_Average_Rate] [6] [0]

[H3C-4 Output_Peak_Rate] [6] [0]

[H3C-5 Output_Average_Rate] [6] [0]

[H3C-22 Priority] [6] [0]

[H3C-60 Ip-Host-Addr] [33] [192.168.47.75 d8:bb:2c:e2:4c:cd]

[46 Acct-Session-Time] [6] [720]

*Jan 23 15:45:42:961 2016 WX5510E RDS/7/DEBUG:

[41 Acct-Delay-Time] [6] [0]

[42 Acct-Input-Octets] [6] [326048]

[47 Acct-Input-Packets] [6] [2108]

[43 Acct-Output-Octets] [6] [2194750]

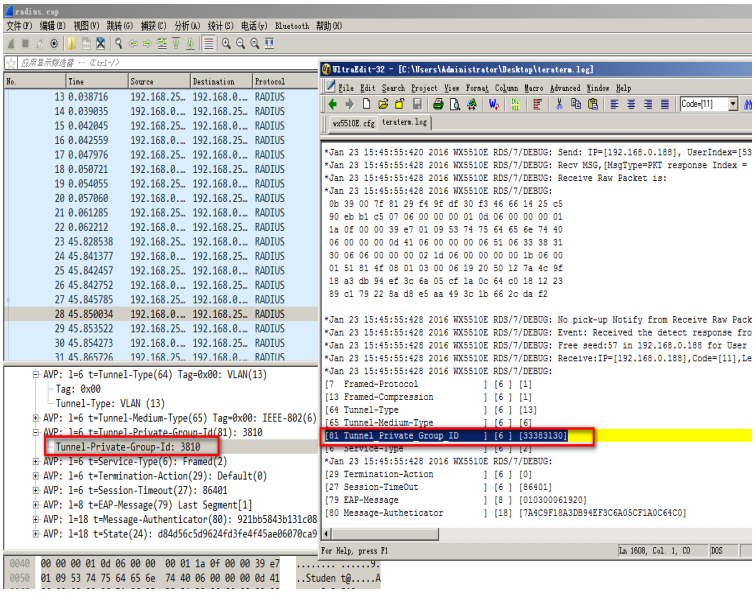
[48 Acct-Output-Packets] [6] [2178]

[52 Acct_Input_Gigawords] [6] [0]

*Jan 23 15:45:42:961 2016 WX5510E RDS/7/DEBUG:

[53 Acct_Output_Gigawords] [6] [0]

可以看到[81 Tunnel_Private_Group_ID 字段下发AC识别为0000002F，而非3810。根据以往要求服务器下发16进制的授权vlan，但用户服务器只能下发字符串，且用户是针对用户名下发的，如果修改为16进制的字符，这个无线用户到其他无线设备上认证时也会有问题。协调抓包发现：



修改第三方服务器下发授权vlan的携带报文为2号

同时设备上配置

vlan 3810

name 3810

识别字符串vlan下发。