某局点无线802.1x逃生不生效的经典案例

802.1X 姜霁琛 2019-03-05 发表

组网及说明

现场无线控制器使用WX3508H，C5417P01版本

问题描述

现场想要配置1x逃生功能，使用命令authentication lan-access radius-scheme xxx none实现，配置后发现，在有线组网中该命令生效了，可以通过该命令实现1x逃生，但是在无线组网中，该命令不生效，当radius认证无效时，不能通过配置的备用认证方式none实现逃生，客户端无法上网。

```
 # domain free1x1
 authentication lan-access radius-scheme free1x none
 authorization lan-access radius-scheme free1x none
 accounting lan-access radius-scheme free1x none
```

确认配置无问题后，查看debug，发现确实在三次尝试radius报文交互失败后，将server处于block状态了。 debug radius可以看到：

```
% Set status of server to block successfully. serverIP: 10.1.1.55, serverPort: 1812.
```

过程分析

802.1x协议从功能上可以分为两大部分：认证部分和密钥协商部分。其中，认证部分需要客户端、设备和认证服务器共同参与，最终完成对客户端的接入认证，特别在WLAN协议中还会在客户端和认证服务器（包括设备）端协商一个radius key，该密钥将被作为后续密钥协商的种子密钥。而密钥协商部分（4-way handshake）只是在设备和客户端之间进行交互，完成对称密钥的协商和生成，生成的密钥最终会作为802.11链路使用的系列密钥。 由此可知，无线1x中继的方式，只有在认证成功后，才会进行4次握手key协商，然后传输加密的数据报文，如果不与服务器交互协商密钥，则下面的步骤无法进行，进而无法加密报文传输。因此中继的方式从协议层面就无法做到逃生。 而chap（终结）结合inode客户端，做的是非加密的，所以该方式可以做逃生操作，但是报文是明文传输并不安全，因此一般的无线1x认证都使用的是中继加密的方法。

所以，我司目前无线1x逃生，在chap的方式下并结合inode客户端可以生效，eap的方式无法生效，现场配置的是eap方式。而chap属于终结方式，不涉及证书认证，并且chap方式必须结合我司inode客户端实现。

解决方法

修改1x认证方式为chap并结合inode之后解决

```
#
wlan service-template 4
ssid free1x
vlan 100
client-security authentication-mode dot1x
dot1x domain free1x1
service-template enable
#
#
domain free1x1
authentication lan-access radius-scheme free1x none
authorization lan-access radius-scheme free1x none
accounting lan-access radius-scheme free1x none
#
#
radius scheme free1x
primary authentication 172.31.3.252
primary accounting 172.31.3.252
key authentication cipher $c$3$zI9cHsibr6OzK+mUhvFN5OjxoPU1tGlb
key accounting cipher $c$3$MUVG3WeorUCni84aGrmNZKHCvPHmvEkG
retry 2
timer quiet 10
timer response-timeout 2
nas-ip 172.31.3.5
#
```