

某局点无线终端IPv6单栈portal认证失败问题处理经验案例

Portal IPv6 殷俊 2018-12-29 发表

组网及说明

客户现网无线业务中存在三个SSID，三个SSID的业务地址组合分别为，IPv4单栈，IPv4+IPv6双栈，IPv6单栈。其中故障业务是IPv6单栈，接入安全采用portal认证，portal server和radius server均为第三方服务器。AC为无线业务启用portal认证。

问题描述

概率性出现IPv6单栈业务portal认证失败，认证失败时portal页可正常推送，输入用户名密码后提示密码错误。

过程分析

AC上开启debug信息查看发现radius server返回access-reject (CODE=3) 认证请求被拒绝，拒绝原因为终端密码错误。

```
*Nov 27 11:17:40:457 2018 AC_4 RADIUS/7/PACKET: Reply-Message="E2901: (Third party 10105015)E2553: Username or password is incorrect."
```

```
*Nov 27 11:17:40:458 2018 AC_4 RADIUS/7/PACKET:
```

```
03 d2 00 5c 0a 71 a3 20 06 d8 70 b1 db ad b7 fe
```

```
eb 4d b6 47 12 48 45 32 39 30 31 3a 20 28 54 68
```

```
69 72 64 20 70 61 72 74 79 20 31 30 31 30 35 30
```

```
31 35 29 45 32 35 35 33 3a 20 55 73 65 72 6e 61
```

```
6d 65 20 6f 72 20 70 61 73 73 77 6f 72 64 20 69
```

```
73 20 69 6e 63 6f 72 72 65 63 74 2e
```

进一步协调radius server排查确认为终端在portal认证时AC发送的radius请求报文access-request报文中携带了双栈地址，既有IPv4地址也有IPv6地址。radius server在该业务portal认证中radius server优先取终端的IPv4地址。但是在用户信息查询中未查到终端的IPv4地址，因此拒绝终端认证接入。

但是为什么IPv6单栈接入情况下AC的radius请求报文access-request报文中会携带IPv4地址。通过反复复现问题，并且通过学习到的IPv4地址段进行分析发现，该IPv4地址是IPv4单栈业务下的地址段，当终端从IPv4单栈无线业务下切换到IPv6单栈无线业务时，部分终端会残留IPv4地址，并未释放。当终端有IPv4地址的arp报文或DHCP续租报文时，AC会学习到终端的IPv4地址，并且当AC学习到无线终端的双栈地址时，默认在radius的access-request报文中会携带双栈地址。

至此，问题最终定位为AC误将无线终端残留的IPv4地址在radius请求报文access-request报文中携带，导致radius server查询失败，拒绝请求。

解决方法

AC上默认开启通过终端发送的arp报文和DHCP报文学习终端的IP地址功能。可以通过以下命令关闭IPv4地址学习功能解决：

```
[WX5540H-V7]wlan service-template 1
```

```
[WX5540H-V7-wlan-st-2]undo client ipv4-snooping arp-learning enable
```

```
[WX5540H-V7-wlan-st-2]undo client ipv4-snooping dhcp-learning enable
```