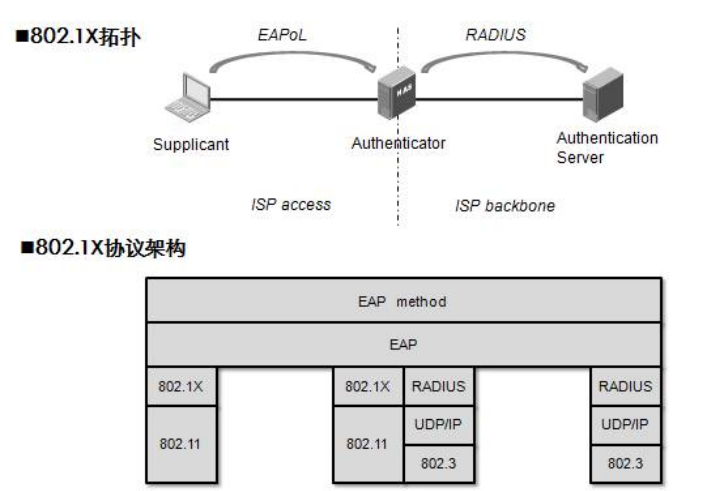
中国移动无感知认证常见问题分析举例

wlan接入 Portal AAA **李晨光** 2012-09-03 发表

中国移动无感知认证常见问题分析举例

一、无感知认证组网&协议架构：

适用于中国移动所有的WLAN组网架构：IAG+AC、纯AC。无感知认证协议架构如下：



AC作为EAP-SIM/PEAP认证点。整个EAP身份认证交换程序在逻辑上是通过申请者与认证服务器来完成的，认证者只是扮演中介的角色。在前端，申请者与认证者之间，使用由802.1X定义的EAP over LAN（EAPoL）协议。在后端，认证者与服务器之间，则是通过RADIUS封包传递EAP报文。最终构建一条从申请者到服务器的认证报文交互通道。

二、问题描述：

中国移动在全国新增EAP-SIM/PEAP业务，即无感知认证业务。由于业务初次上线，移动WLAN用户对该业务尚不熟悉，对终端的操作也不熟练。同时移动后台的认证、计费平台尚在进一步完善当中，导致无感知认证问题复杂多样。该分析案例从AC上的debug radius packet调试信息来定位无感知业务的错误，并列举了常见的无感知认证错误类型。基本涵盖了目前我司AC在开通移动无感知认证时遇到的大部分问题。

无感知认证的AC设备配置并不复杂，配置错误容易检测，这里暂不考虑AC配置问题导致的错误。同时，关于终端的配置错误只考虑一种情况——用户名/密码的错误。

三、问题分析：

无感知认证是通过无线侧的EAPoLAN报文和网络侧的EAPoverRADIUS建立一条从终端到认证服务器的EAP报文交互通道，通过终端用户和认证服务器的信息交互来完成网络侧对WLAN用户的身份认证，EAP-SIM和PEAP是承载于EAP通道上的具体认证方法。AC与服务器侧的RADIUS协议是一个比较标准和通用的协议，而且大部分的认证交互成功与失败的情况都能在RADIUS交互报文中得到体现，因此从AC设备上debug radius packet，能观察到整个认证交互过程。我们先对RADIUS的几类报文做介绍。

Code	报文类型	报文说明
1	Access-Request认证请求包	方向Client->Server，Client将用户信息传输到Server，由Server判断是否接入该用户。该报文中必须包含User-Name属性，可选包含NAS-IP-Address、User-Password、NAS-Port等属性
2	Access-Accept认证接受包	方向Server->Client，如果Access-Request报文中的所有Attribute值都可以接受（即认证通过），则传输该类型报文
3	Access-Reject认证拒绝包	方向Server->Client，如果Access-Request报文中存在任何无法被接受的Attribute值（即认证失败），则传输该类型报文
4	Accounting-Request计费请求包	方向Client->Server，Client将用户信息传输到Server，请求Server开始/停止计费，由该报文中的Acct-Status-Type属性区分计费开始请求和计费结束请求
5	Accounting-Response计费响应包	方向Server->Client，Server通知Client已经收到Accounting-Request报文，并且已经正确记录计费信息

上表列出了5类radius报文：认证请求（Code：1）、认证接受（Code：2）、认证拒绝（Code：3）、计费请求（Code：4）和计费相应（Code：5）。还有一类（Code：11）挑战报文（Access-Challenge），用于在Client和认证服务器之间直接交互，AC只做透传。为了支持EAP中继，radius只是增加了两个扩展属性：EAP-Message（EAP 消息

）和Message-Authenticator（消息认证码）。关于RADIUS属性含义，这里不再赘述。下面分析常见的认证错误。

（1）情况一：RADIUS服务器不响应认证请求。

造成RADIUS服务器不响应的原因有多种，但通过Radius debug信息无法区分具体的类别，需要通过其他方式来判断。常见的原因有：

？ AC和RADIUS网络层不可达；

？ AC发送的RADIUS报文被防火墙阻断，或者服务器回送的报文被丢弃；

？ RADIUS服务器未添加AC的nas-ip，或AC的nas-ip配置不正确；

更具体的明确RADIUS不响应的原因，可以通过其他手段辅助判断，如带nas-ip源ping服务器、tracert等。

Debug情况分析：

搜索code=[1]的报文，发现大量报文重传；同时未发现code=[2]、code=[3]报文（如果AC同时承担PORTAL认证，需要先手动过滤掉PORTAL认证的radius debug报文）。

==========

*Mar 28 09:29:22:091 2012 UBXG-MB-WLAN-AC05-2 RDS/7/DEBUG: Recv MSG,[MsgType=PKT auth timeout Index = 210, ulParam3=0]

*Mar 28 09:29:22:112 2012 UBXG-MB-WLAN-AC05-2 RDS/7/DEBUG: Send: IP=[120.202.164.131], UserIndex=[210], ID=[210], RetryTimes=[1], Code=[1], Length=[263] //认证请求报文（code：1）发生第一次重传。

*Mar 28 09:29:22:132 2012 UBXG-MB-WLAN-AC05-2 RDS/7/DEBUG:

Event: Set socket VPN attribute, VPN index=0, Result=0!

*Mar 28 09:29:25:091 2012 UBXG-MB-WLAN-AC05-2 RDS/7/DEBUG: Recv MSG,[MsgType=PKT auth timeout Index = 210, ulParam3=0]

*Mar 28 09:29:25:112 2012 UBXG-MB-WLAN-AC05-2 RDS/7/DEBUG: Send: IP=[120.202.164.131], UserIndex=[210], ID=[210], RetryTimes=[2], Code=[1], Length=[263] //认证请求报文（code：1）发生第二次重传。

*Mar 28 09:29:25:132 2012 UBXG-MB-WLAN-AC05-2 RDS/7/DEBUG:

Event: Set socket VPN attribute, VPN index=0, Result=0!

#Mar 28 09:29:25:439 2012 UBXG-MB-WLAN-AC05-2 WRRM/4/Channel detected interfere: Channel detected interfere :1.3.6.1.4.1.2011.10.2.75.2.3.0.7 AP Serial Id:210235A22WC119006470 Radio id:1 Channel Number:11

#Mar 28 09:29:25:469 2012 UBXG-MB-WLAN-AC05-2 WRRM/4/AP detected interfere: AP detected interfere :1.3.6.1.4.1.2011.10.2.75.2.3.0.8 AP Serial Id:210235A22WC119006470 Radio id:1 Channel Number:11 APMAC:C4:CA:D9:62:1B:01

%Mar 28 09:29:25:882 2012 UBXG-MB-WLAN-AC05-2 WMAC/6/WMAC_CLIENT_JOIN_WLAN: Client 7c11-bed7-13c3 successfully joins WLAN CMCC-EDU, on APID 70 with BSSID c4ca-d92d-60c1.

%Mar 28 09:29:29:454 2012 UBXG-MB-WLAN-AC05-2 8021X/6/DOT1X_AUTH_FAILURE: -IfName=WLAN-DBSS5:1119-UserName=15717290014; DOT1X authentication failed.

%Mar 28 09:29:29:806 2012 UBXG-MB-WLAN-AC05-2 WMAC/6/WMAC_CLIENT_GOES_OFFLINE: Client 0016-6d7a-2a60 disconnected from WLAN AUTOCMCC-EDU. Reason code is 1.

%Mar 28 09:29:29:826 2012 UBXG-MB-WLAN-AC05-2 PORTSEC/5/PORTSEC_VIOLATION: -IfName=WLAN-DBSS5:1119-MACAddr=00:16:6D:7A:2A:60-VlanId=-1501-IfStatus=Up; Intrusion detected.

%Mar 28 09:29:29:946 2012 UBXG-MB-WLAN-AC05-2 WMAC/6/WMAC_CLIENT_JOIN_WLAN: Client 0016-6d7a-2a60 successfully joins WLAN AUTOCMCC-EDU, on APID 3 with BSSID c4ca-d915-2d32.

%Mar 28 09:29:30:127 2012 UBXG-MB-WLAN-AC05-2 WMAC/6/WMAC_CLIENT_GOES_OFFLINE: Client b8c7-5d7c-e521 disconnected from WLAN CMCC-EDU. Reason code is 8.

*Mar 28 09:29:30:304 2012 UBXG-MB-WLAN-AC05-2 RDS/7/DEBUG: Recv MSG,[MsgType=PKT auth timeout Index = 210, ulParam3=0]

*Mar 28 09:29:30:404 2012 UBXG-MB-WLAN-AC05-2 RDS/7/DEBUG:

Event: Begin to switch RADIUS server when sending 0 packet.

*Mar 28 09:29:30:534 2012 UBXG-MB-WLAN-AC05-2 RDS/7/DEBUG: The RD TWL timer has resumeed.

*Mar 28 09:29:30:615 2012 UBXG-MB-WLAN-AC05-2 RDS/7/DEBUG:

Event: No active RADIUS server is available for switching when sending packet (pkt-flag = 0).

*Mar 28 09:29:30:788 2012 UBXG-MB-WLAN-AC05-2 RDS/7/DEBUG:

Error: Auth server no response.(AAAID = 210, Req-ID = 0) //报错：RADIUS服务器不可达

*Mar 28 09:29:30:908 2012 UBXG-MB-WLAN-AC05-2 RDS/7/DEBUG: RADIUS Server No Response

==========

（2）情况二：用户帐号不正确，即无效帐号。（适用于PEAP认证）

用户帐号无效有可能是用户输入的帐号信息错误，或者终端配置错误上送错误的用户名，比如window系统做PEAP认证时未去掉“自动使用Windows登录名和密码”选项。

Debug情况分析：

搜索code=[3]的报文，code=[3]为认证拒绝报文，message消息中携带具体的错误消息：“user not found in db”。

==========

*Jul 4 17:40:09:098 2012 SDQDA-WLAN-AC141-HSWX6108-AC1 RDS/7/DEBUG: Recv MSG,[MsgType=PKT response Index = 129, ulParam3=3238036976]

*Jul 4 17:40:09:099 2012 SDQDA-WLAN-AC141-HSWX6108-AC1 RDS/7/DEBUG: Receive Raw Packet is:

*Jul 4 17:40:09:099 2012 SDQDA-WLAN-AC141-HSWX6108-AC1 RDS/7/DEBUG:

03 81 00 81 2e 55 c4 c2 1f a9 be 4f 4b da d2 3e

e6 21 f8 8d 4f 06 04 0a 00 04 12 55 33 39 3b 45

61 70 20 41 75 74 68 65 6e 74 69 63 61 74 69 6f

6e 20 46 61 69 6c 65 64 2c 20 75 73 65 72 20 6e

6f 74 20 66 6f 75 6e 64 20 69 6e 20 64 62 2c 20

52 65 71 75 65 73 74 20 44 65 6e 79 20 62 79 20

63 68 69 6e 61 6d 6f 62 69 6c 65 2e 63 6f 6d 50

12 a5 38 58 ee 11 be fb 16 41 17 65 bd eb 57 f5

f2

*Jul 4 17:40:09:099 2012 SDQDA-WLAN-AC141-HSWX6108-AC1 RDS/7/DEBUG: No pick-up Notify from Receive Raw Packet!

*Jul 4 17:40:09:099 2012 SDQDA-WLAN-AC141-HSWX6108-AC1 RDS/7/DEBUG: Receive:IP=[221.176.1.138],Code=[3],Length=[129]

*Jul 4 17:40:09:099 2012 SDQDA-WLAN-AC141-HSWX6108-AC1 RDS/7/DEBUG:

[79 EAP-Message] [6] [040A0004]

[18 Reply-Message] [85] [39;Eap Authentication Failed, user not found in db, Request Deny by chinamobile.com] //radius拒绝原因为：数据库系统未查询到该帐号。

[80 Message-Autheticator] [18] [A53858EE11BEFB16411765BDEB57F5F2]

*Jul 4 17:40:09:100 2012 SDQDA-WLAN-AC141-HSWX6108-AC1 RDS/7/DEBUG: Reject

Msg=[39;Eap Authentication Failed, user not found in db, Request Deny by chinamobile.com]

%Jul 4 17:40:09:100 2012 SDQDA-WLAN-AC141-HSWX6108-AC1 8021X/6/DOT1X_AUTH_FAILURE: -IfName=WLAN-DBSS30:443-UserName=18500000100; DOT1X authentication failed.

#Jul 4 17:40:09:102 2012 SDQDA-WLAN-AC141-HSWX6108-AC1 WMAC/4/Station Authorization Fail: Station Auth Fail:1.3.6.1.4.1.2011.10.2.75.3.2.0.3 StaMac1:00:22:FB:19:BC:B2 StaMac2:00:22:FB:19:BC:B2 UserName:18500000100 StaMac3:00:22:FB:19:BC:B2 Radioid:1 SSIDName:CMCC-AUTO Cause:1 Desc:Unknown Failure APID:210235A0D4C11A025505 BSSID:C4:CA:D9:81:E3:B0 AuthMode: 1

%Jul 4 17:40:09:102 2012 SDQDA-WLAN-AC141-HSWX6108-AC1 PORTSEC/6/PORTSEC_DOT1X_LOGIN_FAILURE: -IfName=WLAN-DBSS30:443-MACAddr=00:22:FB:19:BC:B2-VlanId=3000-UserName=18500000100; The user failed the 802.1X authentication.

%Jul 4 17:40:09:103 2012 SDQDA-WLAN-AC141-HSWX6108-AC1 WMAC/6/WMAC_CLIENT_GOES_OFFLINE: Client 0022-fb19-bcb2 disconnected from WLAN CMCC-AUTO. Reason code is 1.

%Jul 4 17:40:09:170 2012 SDQDA-WLAN-AC141-HSWX6108-AC1 PORTSEC/5/PORTSEC_VIOLATION: -IfName=WLAN-DBSS30:443-MACAddr=00:22:FB:19:BC:B2-VlanId=-3000-IfStatus=Up; Intrusion detected.

==========

（3）情况三：密码错误（适用于PEAP认证）。

PEAP密码错误时，并不会产生code=[3]的radius拒绝报文，而是服务器直接通过code=[11]的鉴权报文通告终端，提示鉴权信息验证失败，终端上会很快提示认证失败（具体的错误信息与终端类型相关）。

Debug情况分析：

搜索code=[11]的报文，最后一条code=[11]报文会携带错误信息：“MSCHAPV2_FAILURE”。

==========

*Aug 20 11:38:15:880 2012 GSLZ-MA-WLAN-RJJD-AC4-JQL-H3C RDS/7/DEBUG: Receive:IP=[221.176.1.138],Code=[11],Length=[179]

*Aug 20 11:38:15:881 2012 GSLZ-MA-WLAN-RJJD-AC4-JQL-H3C RDS/7/DEBUG:

[79 EAP-Message] [109] [010B006B1900170301006086100BD61D9ED6C2FA7AF2A95595CA22E3D9690894839367B5C49B8F6296CB1F18418994818D7B06D64B3DE318629D1E42B574EC10F6C01A396ED9F5EA0CD6EDD4C6FED548EFBE2E1C2917486705D3858DD8F81A8581382C8DFD8A46A9D1786F]

[24 State] [10] [843B558D00027A7A]

[18 Reply-Message] [22] [MSCHAPV2_FAILURE_REQ]

[80 Message-Autheticator] [18] [A3B8692EE27DD7837BBA2A42D16B4854]

*Aug 20 11:38:15:881 2012 GSLZ-MA-WLAN-RJJD-AC4-JQL-H3C RDS/7/DEBUG: Event: Received Access-Challenge pkt.

*Aug 20 11:38:15:882 2012 GSLZ-MA-WLAN-RJJD-AC4-JQL-H3C RDS/7/DEBUG: Event: Succeeded in processing Access-Challenge pkt.

*Aug 20 11:38:15:883 2012 GSLZ-MA-WLAN-RJJD-AC4-JQL-H3C 8021X/7/EVENT: Auth: 119,Msg: ACM authentication continue.

*Aug 20 11:38:15:883 2012 GSLZ-MA-WLAN-RJJD-AC4-JQL-H3C 8021X/7/EVENT: Port: WLAN-DBSS10:139,Auth:119,Received Msg:20482, Current state:14

*Aug 20 11:38:15:884 2012 GSLZ-MA-WLAN-RJJD-AC4-JQL-H3C 8021X/7/PACKET: Port :WLAN-DBSS10:139,Transmitted a packet.

---Verbose information of the packet---

Destination Mac Address: 5cac-4c7d-841d

Source Mac Address: c4ca-d97b-3102

Mac Frame Type: 888e.

Protocol Version ID: 1.

Packet Type: 0.

Packet Length: 107.

-----Packet Body-----

Code: 1.

Identifier: b.

Length: 107.

%Aug 20 11:38:15:894 2012 GSLZ-MA-WLAN-RJJD-AC4-JQL-H3C WMAC/6/WMAC_CLIENT_GOES_OFFLINE: Client 5cac-4c7d-841d disconnected from WLAN CMCC-AUTO. Reason code is 8.

*Aug 20 11:38:15:894 2012 GSLZ-MA-WLAN-RJJD-AC4-JQL-H3C 8021X/7/EVENT: Port: WLAN-DBSS10:139,Notify 1x User offline.

*Aug 20 11:38:15:895 2012 GSLZ-MA-WLAN-RJJD-AC4-JQL-H3C 8021X/7/EVENT: Auth: 119,

*Aug 20 11:38:15:896 2012 GSLZ-MA-WLAN-RJJD-AC4-JQL-H3C 8021X/7/EVENT: Port: WLAN-DBSS10:139,Auth:119,Received Msg:32, Current state:14

*Aug 20 11:38:15:896 2012 GSLZ-MA-WLAN-RJJD-AC4-JQL-H3C 8021X/7/EVENT: Auth: 119,Processing node FAILURE...

*Aug 20 11:38:15:897 2012 GSLZ-MA-WLAN-RJJD-AC4-JQL-H3C 8021X/7/EVENT: Port: WLAN-DBSS10:139,Auth:119,Processing node Unauthor action...

*Aug 20 11:38:15:897 2012 GSLZ-MA-WLAN-RJJD-AC4-JQL-H3C 8021X/7/EVENT: Auth: 119,Sending EAPoL-Failure...

==========

（4）情况四：用户未开通业务（适用于SIM认证）。

对于SIM认证，不需要手动输入用户名、密码。AAA通过后台和HLR/GGSN交互获取用户的鉴权信息完成对用户的认证。如果用户的手机号未开通SIM认证，则必然造成认证失败。

Debug情况分析：

搜索code=[3]的报文，code=[3]为认证拒绝报文，message消息中携带具体的错误消息：“Illegal Account”。

==========

*Apr 6 17:50:29:645 2012 GDGZ-MA-WLAN-HS-0124-QHD-AC RDS/7/DEBUG: Receive Raw Packet is:

*Apr 6 17:50:29:645 2012 GDGZ-MA-WLAN-HS-0124-QHD-AC RDS/7/DEBUG:

03 96 00 8c 0e 5e 56 f6 31 40 4f 05 7f 01 47 98

33 60 a7 4c 12 78 31 38 3b 55 73 65 72 28 35 45

41 38 32 43 42 36 34 30 43 45 36 34 31 38 43 31

35 39 42 29 20 43 68 65 63 6b 69 6e 67 20 4c 6f

67 69 6e 55 73 65 72 20 52 42 69 6c 6c 53 65 72

76 65 72 2c 20 72 65 74 75 72 6e 20 49 6c 6c 65

67 61 6c 20 41 63 63 6f 75 6e 74 2c 20 52 65 71

75 65 73 74 20 44 65 6e 79 20 62 79 20 63 68 69

6e 61 6d 6f 62 69 6c 65 2e 63 6f 6d

*Apr 6 17:50:29:646 2012 GDGZ-MA-WLAN-HS-0124-QHD-AC RDS/7/DEBUG: No pick-up Notify from Receive Raw Packet!

*Apr 6 17:50:29:646 2012 GDGZ-MA-WLAN-HS-0124-QHD-AC RDS/7/DEBUG: Receive:IP=[221.176.1.138],Code=[3],Length=[140]

*Apr 6 17:50:29:646 2012 GDGZ-MA-WLAN-HS-0124-QHD-AC RDS/7/DEBUG:

[18 Reply-Message] [120] [18;User(5EA82CB640CE6418C159B) Checking Login User RBillServer, return Illegal Account, Request Deny by chinamobile.com] //radius拒绝原因为：帐号非法。

*Apr 6 17:50:29:646 2012 GDGZ-MA-WLAN-HS-0124-QHD-AC RDS/7/DEBUG: RejectMsg=[18;User(5EA82CB640CE6418C159B) Checking LoginUser RBillServer, return Illegal Account, Request Deny by chinamobile.com]

%Apr 6 17:50:29:646 2012 GDGZ-MA-WLAN-HS-0124-QHD-AC 8021X/6/DOT1X_AUTH_FAILURE: -IfName=WLAN-DBSS4:128-UserName=5EA82CB640CE6418C159B; DOT1X authentication failed.

==========

（5）情况五：用户帐号余额不足。

移动无感知业务存在5分钟试用的机制，5分钟之后，账户余额清零。如需继续使用，就需要付费申请正式开通无感知业务。当帐号欠费时，认证失败。

Debug情况分析：

搜索code=[3]的报文，code=[3]为认证拒绝报文，message消息中携带具体的错误消息：“Credit is ZERO”。

==========

*Aug 31 18:16:15:239 2012 HEHAD-WLAN-AC01-HSWX6103 RDS/7/DEBUG: Receive Raw Packet is:

*Aug 31 18:16:15:249 2012 HEHAD-WLAN-AC01-HSWX6103 RDS/7/DEBUG:

03 84 00 81 f5 ea b9 5c 9f 73 96 10 e5 e4 4b 04

b0 4b 47 0a 12 6d 31 38 3b 55 73 65 72 28 31 33

34 38 33 34 30 39 38 33 38 29 20 43 68 65 63 6b

69 6e 67 20 4c 6f 67 69 6e 55 73 65 72 20 52 42

69 6c 6c 53 65 72 76 65 72 2c 20 72 65 74 75 72

6e 20 43 72 65 64 69 74 20 69 73 20 5a 45 52 4f

2c 20 52 65 71 75 65 73 74 20 44 65 6e 79 20 62

79 20 63 68 69 6e 61 6d 6f 62 69 6c 65 2e 63 6f

6d

*Aug 31 18:16:15:300 2012 HEHAD-WLAN-AC01-HSWX6103 RDS/7/DEBUG: Event: Received the detect response from auth-server(IP:221.176.1.138).

*Aug 31 18:16:15:370 2012 HEHAD-WLAN-AC01-HSWX6103 RDS/7/DEBUG: No pick-up Notify from Receive Raw Packet!

*Aug 31 18:16:15:475 2012 HEHAD-WLAN-AC01-HSWX6103 RDS/7/DEBUG: Free seed: 132 in 221.176.1.138 for User ID:2589

*Aug 31 18:16:15:596 2012 HEHAD-WLAN-AC01-HSWX6103 RDS/7/DEBUG: Receive:IP=[221.176.1.138],Code=[3],Length=[129]

*Aug 31 18:16:15:716 2012 HEHAD-WLAN-AC01-HSWX6103 RDS/7/DEBUG:

[18 Reply-Message] [109] [18;User(13483409838) Checking LoginUser RBillServer, return Credit is ZERO, Request Deny by chinamobile.com] //radius拒绝原因为：Credit is ZERO

*Aug 31 18:16:15:917 2012 HEHAD-WLAN-AC01-HSWX6103 RDS/7/DEBUG: RejectMsg=[18;User(13483409838) Checking LoginUser RBillServer, return Credit is ZERO, Request Deny by chinamobile.com]

四、总结：

移动的无感知认证错误种类较多，大都可以通过debug radius信息来分析定位。本案例列举的常见错误汇总如下：

（1）RADIUS服务器不响应认证请求；

（2）用户帐号不正确，即无效帐号。（适用于PEAP认证）；

（3）密码错误（适用于PEAP认证）；

（4）用户未开通业务（适用于SIM认证）；

（5）用户帐号余额不足；