设备管理某某某年最新中国移动无线局域网设备测试规

－ ××××-××-××发布

中国移动无线局域网（WLAN）AP、AC设备测试规范-认证及计费分册

目录

前言

本标准的目的是制定中国移动 WLANAPAC 设备的测试要求。

本标准是 WLAN 测试规范三个分册之一。本次修订把 WLANAP、AC 测试规范分为三个分册，《中国移动无线局域网（WLAN）AP、AC 设备测试规范-射频与性能分册》、《中国移动无线局域网（WLAN）AP、AC 设备测试规范-功能分册》、《中国移动无线局域网（WLAN）AP、AC 设备测试规范-认证及计费分册》。

本标准是 WLAN 系列标准之一，该系列标准的结构、名称或预计的名称如下：

序号,标准编号,标准名称
[1],QB-D-055-2010,中国移动无线局域网（WLAN）业务规范
[2],QB-D-056-2010,中国移动无线局域网（WLAN）业务总体技术要求
[3],QB-A-016-2010,中国移动无线局域网（WLAN）AP、AC 设备规范
[4],QB-A-017-2010,中国移动无线局域网（WLAN）Portal、Radius 设备规范
[5],QB-A-018-2010,中国移动无线局域网（WLAN）设备接口规范
[6],QB-A-019-2010,中国移动无线局域网（WLAN）用户接入流程技术规范
[7],QB-A-020-2010,中国移动无线局域网（WLAN）AP、AC 设备测试规范
[8],QB-A-021-2010,中国移动无线局域网（WLAN）Portal、Radius 设备测试规范
[9],QB-D-057-2010,中国移动无线局域网（WLAN）用户界面规范
[10],QB-E-021-2010,中国移动无线局域网（WLAN）客户端规范
[11],QB-E-022-2010,中国移动无线局域网（WLAN）终端技术规范
[12],QB-E-023-2010,中国移动无线局域网（WLAN）终端测试规范
[13],QB-W-033-2010,中国移动无线局域网（WLAN）网络管理总体技术要求
[14],QB-W-034-2010,中国移动无线局域网（WLAN）网络管理功能要求
[15],QB-W-035-2010,中国移动无线局域网（WLAN）设备网管接口技术规范
[16],QB-W-036-2010,中国移动无线局域网（WLAN）设备网管接口测试规范

本标准由中移技号文件印发。

本标准由中国移动通信集团计划建设部提出，集团公司技术部归口。

本标准起草单位：中国移动通信有限公司研究院

本标准主要起草人：钟大平、邸志宇、邵春菊、陈超、韩瑜

1. 范围

本标准规定了中国移动 WLAN 接入设备测试要求，供中国移动内部和厂商共同使用；适用于中国移动开展 WLAN 业务所涉及到的 WLAN 接入设备测试。

2. 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

表 2-1 规范性引用文件

序号,标准编号,标准名称,发布单位

[1],QB-D-056-2010,中国移动无线局域网（WLAN）业务总体技术要求,中国移动通信集团公司

[2],QB-A-016-2010,中国移动无线局域网（WLAN）AP、AC 设备规范,中国移动通信集团公司

[3],QB-A-018-2010,中国移动无线局域网（WLAN）设备接口规范,中国移动通信集团公司

[4],QB-C-008-2012,中国移动无线局域网（WLAN）用户接入流程技术规范,中国移动通信集团公司

3. 术语、定义和缩略语

下列术语、定义和缩略语适用于本标准：

表 3-1 缩略语

词语,解释

3GPP,3rdGenerationPartnershipProject

AAA,Authentication，Authorization，Accounting

AC,AccessController

ACL,AccessControlList

ACK,Acknowledgement

AES,AdvancedEncryptionStandard

AP,AccessPoint

A-MPDU,AggregateMACProtocolDataUnit

A-MSDU,AggregateMACServiceDataUnit

AKA,AuthenticationAndKeyAgreement

ARP,AddressResolutionProtocol

AS,AuthenticationServer

BOSS,BusinessOperationSupportSystem

BWr,ReferenceBandwidth

CAR,CommittedAccessRate

CCK,ComplementaryCodeKeying

CCMP,CounterCBC-MACProtocol

CDN,CouplingDecouplingNetwork

CMCC,ChinaMobileCommunicationsCorporation

CHAP,ChallengeHandshakeAuthenticationProtocol

CMNET,ChinaMobileNet

CW,ContinuousWave

DBPSK,DifferentialBinaryPhaseShiftKeying

DCS,DigitalCellularSystem

DFS,DynamicFrequencySelection

DHCP,DynamicHostConfigurationProtocol

DNS,DomainNameServer

DoS,DenialOfService

DQPSK,DifferentialQuadraturePhaseShiftKeying

DSCP,DifferentiatedServicesCodePoint

DSSS,DirectSequenceSpreadSpectrum

DUT,DeviceUnderTest

EAP,ExtensibleAuthenticationProtocol

EAPOL,EAPOverLan

FTP,FileTransferProtocol

GSM,GlobalSystemForMobileCommunication

HTTP,HyperTextTransportProtocol

HTTPS,HyperTextTransportProtocolSecure

HLR,HomeLocationRegister

HT,HighThroughput

ICMP,InternetControlMessagesProtocol

IE,InformationElement/WindowsInternetExplorer

IP,InternetProtocol

LAN,LocalAreaNetwork

LTE,LongTermEvolution

MAC,MediaAccessControl

MCS,ModulationandCodingScheme

MIB,ManagementInformationBase

MIMO,MultipleInput,MultipleOutput

MPDU,MACProctolDataUnit

MS-CHAP,Microsoft-ChallengeHandshakeAuthenticationProtocol

MSDU,MACServiceDataUnit

NAT,NetworkAddressTranslation

NTP,NetworkTimeProtocol

OBW,OccupiedBandWidth

OFDM,OrthogonalFrequencyDivisionMultiplexing

PAP,PasswordAuthenticationProtocol

PAT,PortAddressTranslation

PC,PersonalComputer

PEAP,ProtectedExtensibleAuthenticationProtocol

PER,PacketErrorRate

PLCP,PhysicalLayerConvergenceProtocol

POE,PoweroverEthernet

PPM,PartsPerMillion

PPPoE,Point-to-PointProtocoloverEthernet

PSDU,PowerSwitchingDistributionUnit

PSK,PreSharedKey

QoS,QualityofService

RADIUS,RemoteAuthenticatonDialInUserService

RF,RadioFrequency

SCP,ServiceControlPoint

Short-GI,ShortGuardInterval

SLAAC,StatelessAddressAutoconfiguration

SISO,SingleInput,SingleOutput

SNMP,SimpleNetworkManagementProtocol

SSID,ServiceSetIdentifier

STA,Station

TD,TimeDivision

TKIP,TemporalKeyIntegrityProtocol

TPC,TransmitPowerControl

UE,UserEquipment

VLAN,VirtualLocalAreaNetwork

VOD,Video-On-Demand

VPN,VirtualPrivateNetwork

WAPI,WirelessLANAuthenticationandPrivacyInfrastructure

WEP,WiredEquivalentPrivacy

WLAN,WirelessLAN

WPA,Wi-FiProtectedAccess

4. 测试环境

4.1. 总体测试示意图

测试环境如图 4-1 所示。图 4-1 仅为示意图，并不代表实际组网结构。

图 4-1WLAN 测试组网图

4.2. 接入流程测试组网图

图 4-2 接入流程测试组网图

5. 测试仪器以及软件列表

5.1. 测试仪器列表

表 5-1 测试仪器列表

仪器名称,数量,单位,备注

AC 流量测试仪,1,台,AC 性能测试

AC 隧道协议仿真器,1,台,仿真 AC-AP 隧道报文

AP 流量测试工具,1,套,IxChariot

AP 用户模拟工具,1,台,模拟接入 AP 的多个用户行为

频谱分析仪,1,台,完成 WLAN 信号的频域、时域分析

信号发生器,1,台,产生模拟 WLAN 信号、干扰信号。

综合测试仪,1,台,矢量信号解析，包括功率、EVM 等

数字电源,2,台,

5.2. 测试辅助设备列表

表 5-2 测试辅助设备列表

仪器名称,数量,单位,备注

PC,1,台,作为网管服务器，需要较高性能

便携电脑,若干,台,能够支持 802.11i/WAPI

不同厂家的无线网卡(包括内置网卡),至少 4,块,支持 802.11ag/n 模式;能够支持:WMMWPA2/WAPI。

需要多块网卡是为了测试 AP 与不同网卡的兼容性

交换机,1,台,Layer2,用于抓包

3GPPAAA,1,台,用于 EAP-SIM/EAP-AKA 认证测试

HLR,1,台,用于 EAP-SIM/EAP-AKA 认证测试

SIM 卡,5,张,

POE 供电模块,1,块,

长网线,10,根,7 米、10 米、20 米-90 米

双模无线网卡,1,块,用于 EAP-SIM/EAP-AKA 认证测试

衰减器,若干,个,可调衰减器

RF 电缆,若干,条,频率范围 9KHz~12.75GHz

功率计,1,台,测量信号的功率

手机,若干,部,

5.3. 测试软件列表

表 5-3 测试软件列表

软件名称,数量,单位,备注

VODServer,1,个,

DHCPServer,1,个,

FTPServer/Client,1,个,Serv-U/CuteFTP

WEBServer,1,个,

多播服务器,1,台,

MIBBrowser,1,个,网管相关

Portal AAAserver,1,个,Portal 及无感知认证

DoS 攻击软件,1,套,用于防 DoS 攻击测试

抓包软件,2,套,用于有线抓包和无线抓包

随 e 行客户端软件,1,套,注:研究院提供

iPass 客户端软件,1,套,注:研究院提供

PPPoE 拨号软件,1,套,

6. 测试项目优先级说明

根据产品入网测试实际需求,所有测试项目分为 3 类:基本要求、重要要求、可选要求。

✓ 基本要求:最基本的需求,设备若缺少该要求,则网络难以运行或提供业务;

✓ 重要要求：增强型的需求，应用场景较广泛，设备若支持该要求，可获得较明显的增益；

✓ 可选要求：长期关注的需求/当前需求不强烈，具有一定的应用场景，设备若支持该要求，可获得一定的增益。

7. 测试用例

7.1. 认证功能测试

7.1.1. WEB 认证

7.1.1.1. AC 支持连接多个 Portal/Radius 服务器功能

项目:,WEB 认证,分项目:,AC 支持连接多个 Portal/Radius 服务器功能

用例编号:,7.1.1.1,版本:,2.0.0

参考文档:,无,参考组网:,无

重要性:,基本要求,优先级:,A

测试目的:,检验 AC 可以根据不同的 SSID 指向不同的 Portal/Radius 服务器进行认证

1. 预置条件:,配置多个（至少 2 个）Portal 服务器和 Radius 服务器，并保证 STA 与各 Portal/Radius 服务器 IP 可达；

2. 在 AC 上配置 SSID1 对应 Portal1/Radius1 服务器，SSID2 对应 Portal2/Radius2 服务器；

3. WLAN 用户可以正常接入无线网络。

1. 测试步骤:,无线用户通过 SSID1 接入无线网络；

2. 打开浏览器，在地址栏中输入一个外网地址；

3. 无线用户通过 SSID2 接入无线网络；

4. 打开浏览器，在地址栏中输入一个外网地址。

1. 预期结果:,步骤 2，无线用户通过 Portal1 服务器推出认证页面，并通过 Radius1 服务器完成认证。

2. 步骤 4，无线用户通过 Portal2 服务器推出认证页面，并通过 Radius2 服务器完成认证。

1. 备注：,此测试项属于中国移动集团客户 WLAN 业务测试项。

7.1.1.2. AC 支持在 Portal 重定向的 URL 中携带 SSID 信息

项目:,WEB 认证,分项目:,AC 支持在 Portal 重定向的 URL 中携带 SSID 信息

用例编号:,7.1.1.2,版本:,2.0.0

参考文档:,无,参考组网:,无

重要性:,基本要求,优先级:,A

测试目的:,检验 AC 对 Portal 重定向的 URL 中携带 SSID 信息的支持能力

1. 预置条件:,用户已获取了密码，并开通了相应的业务；

2. 已经正确安装网卡；

3. WLAN 用户申请 IP 地址正常；

4. WLAN 接入系统 WEB 认证功能配置正确。

1. 测试步骤:,WLAN 用户申请 IP 地址；

2. WLAN 用户访问 WWW 服务器。

1. 预期结果:,步骤 2 中终端无法访问 WWW 服务器，被强制到 Portal 服务器上。

2. 步骤 2 中 AC 需要在 Portal 重定向的 URL 中携带 SSID 信息。

1. 备注：,SSID 参数的相关约定：

参数名要求是小写字母串“ssid”

参数值为 32 位字符串，且字符要求是字母或数字

当 AC 指向 PORTAL 时，参数“ssid”要求追加在 URL 串的最后，如?wlanuserip=10.1.2.34&wlanacname=.&ssid=CMCC-Starbucks

此测试项属于中国移动集团客户 WLAN 业务测试项。

7.1.1.3. AC 支持长用户名认证的能力

项目:,WEB 认证,分项目:,AC 支持长用户名认证的能力

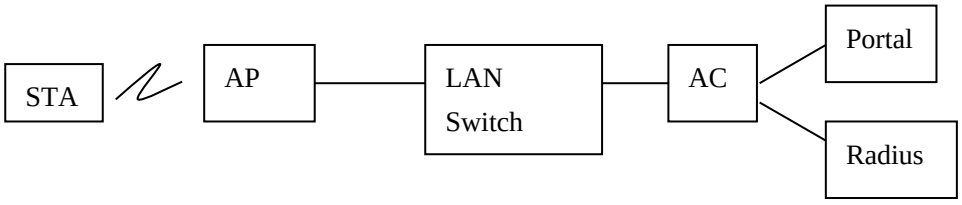
用例编号:,7.1.1.3,版本:,2.0.0

参考文档:,无,参考组网：,参见预置条件

重要性:,基本要求,优先级:,A

测试目的:,检验 AC 对长用户名认证的支持能力，保证国际漫游用户的正常认证

预置条件:,参考组网：



1. 设置用户名为“890……123”，（由 890 循环构成，共 253 字节），并开通了相应的业务；

2. 已经正确安装网卡；

3. WLAN 用户申请 IP 地址正常；

4. WLAN 接入系统 WEB 认证功能配置正确。

1. 测试步骤:,使用长用户名的用户关联到 WLAN 网络；

2. 打开 IE，输入用户名和密码进行 WEB 认证；

3. 观察 AC 所能支持的最长用户名。

1. 预期结果:,在步骤 2 中，终端通过认证。

2. 在步骤 3 中，记录 AC 所能支持的最长用户名。

1. 备注：,通常为 253 字节。

7.1.1.4. AC 支持白名单配置的能力

项目:,WEB 认证,分项目:,AC 支持白名单配置的能力

用例编号:,7.1.1.4,版本:,2.0.0

参考文档:,无,参考组网：,参见预置条件

重要性:,基本要求,优先级:,A

测试目的:,检验 AC 对白名单配置的支持能力

预置条件:,参考组网：

1. 用户已获取了密码，并开通了相应的业务；

2. 已经正确安装网卡；

3. WLAN 用户申请 IP 地址正常；

4. WLAN 接入系统 WEB 认证功能配置正确。

1. 测试步骤:,AC 上配置 32 个白名单地址；

2. WLANUE 申请 IP 地址；

3. 使用 WLANUE 上的浏览器访问因特网，访问 AC 配置在白名单中的地址。

1. 预期结果:,步骤 1 中 AC 至少可以配置 32 个白名单地址。

2. 步骤 3 中终端在认证前可以正常访问 AC 配置在白名单中的地址。

1. 备注：,需要记录 AC 最多可以配置的白名单数目，是否可以配置 IP 段及端口。

7.1.1.5. 主备 Radius 用户认证服务器倒换支持

项目:,WEB 认证,分项目:,主备 Radius 用户认证服务器倒换支持

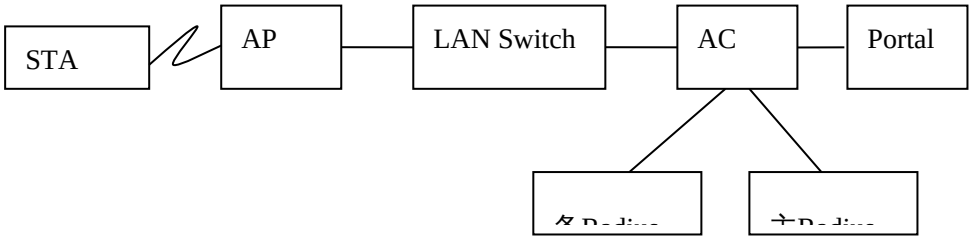
用例编号:,7.1.1.5,版本:,2.0.0

参考文档:,无,参考组网:,参见预置条件

重要性:,基本要求,优先级:,A

测试目的:,检验 WLAN 接入系统支持主备 Radius 用户认证服务器倒换支持机制

预置条件:,参考组网：



1. 用户已获取了密码，并开通了相应的业务；
2. 已经正确安装网卡；
3. WLAN 用户申请 IP 地址正常；
4. WLAN 接入系统 WEB 认证功能配置正确，并同时配置了主备两台 Radius 认证服务器。

1. 测试步骤:,终端用户连接 WLAN 网络；
2. 终端用户打开 IE，输入正确的用户名和密码进行 WEB 认证；
3. 观察用户的认证和计费情况。连续 PingWWW 服务器，观察连接状况；
4. 断开主 Radius 认证服务器和网络的连接，观察用户连接及业务状况；
5. 断开用户连接，重新接入到 WLAN 网络；
6. 观察用户的认证和计费情况。

1. 预期结果:,在步骤 2 中，终端用户通过 WEB 认证。
2. 在步骤 3 中，可以在主 Radius 认证/计费服务器上观察到用户的认证和计费信息。
3. 在步骤 4 中，用户的网络连接及上层应用不会中断；可以在备 Radius 认证/计费服务器上观察到用户的认证和计费信息。
4. 在步骤 5 中，终端用户通过 WEB 认证。
5. 在步骤 6 中，可以在备 Radius 认证/计费服务器上观察到用户的认证和计费信息。

1. 备注：,主备 Radius 倒换期间用户连接不应发生中断，不需要用户重新认证；
2. 设备倒换期间计费话单格式要与未倒换前完全一致。

7.1.1.6. AP 限制最大接入用户数的能力

项目:,WEB 认证,分项目:,AP 限制最大接入用户数的能力

用例编号:,7.1.1.6,版本:,2.0.0

参考文档:,无,参考组网:,参见预置条件

重要性:,基本要求,优先级:,A

测试目的:,检验 AP 限制最大关联、接入用户数的能力

预置条件:,参考组网：

1. 用户已获取了密码，并开通了相应的业务；

2. 已经正确安装网卡；

3. WLAN 用户申请 IP 地址正常；

4. WLAN 接入系统 WEB 认证功能配置正确。

1. 测试步骤:,配置 AP 最大关联用户数为 2 个；

2. 终端 1、终端 2 关联到 WLAN 网络；

3. 终端 1、2 打开 IE，输入正确的用户名和密码进行 WEB 认证；

4. 终端 3 关联到 WLAN 网络并进行认证，观察结果；

5. 修改 AP 最大关联用户数为 3 个，重复测试步骤 2、3；

6. 观察终端 4 的关联和认证结果。

1. 预期结果:,在步骤 3 中，终端 3 无法关联到 AP。

2. 在步骤 6 中，终端 1-3 正常连接并通过认证；终端 4 无法关联到 AP。

备注：,

7.1.2. 不同 SSID 混合认证

7.1.2.1. 混合接入认证（WebPortal/PEAP/SIM 认证）

项目:,不同 SSID 混合认证,分项目:,混合接入认证（WebPortal/PEAP/SIM 认证）

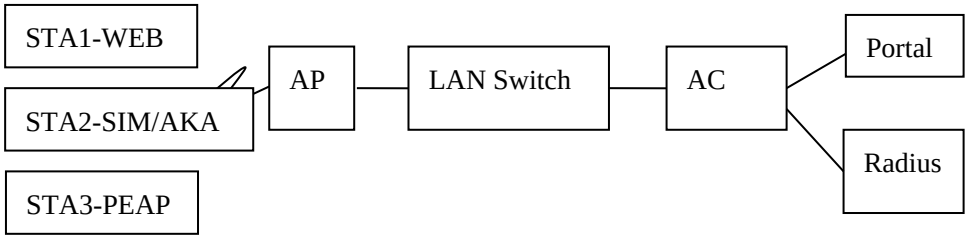
用例编号:,7.1.2.1,版本:,2.0.0

参考文档:,无,参考组网:,参见预置条件

重要性:,基本要求,优先级:,A

测试目的:,检验 WLAN 接入系统能够同时支持多种接入认证方式（WebPortal、PEAP 和 SIM 认证）

预置条件:,参考组网：



1. 配置两个 SSID，一个为 CMCC（配置 WebPortal 认证方式，不加密），另一个为 CMCC-AUTO（配置 PEAP 认证和 SIM 认证共存，均采用 WPA2 加密）；

2. WLAN 接入系统配置正确；

3. 不同类型用户认证服务器分别配置正确并连接正确；

4. 相应的接入认证客户端软件成功安装；

5. 各系统正常运行。

1. 测试步骤:,开启 3 台 WLAN 接入终端（终端 1 为 PC，终端 2 和终端 3 为手机），分别采用 WEB、EAP-SIM/EAP-AKA、PEAP-MSCHAPv2 接入认证方式；

2. 依次接入这 3 种不同认证类型的用户终端并进行认证，整个过程需抓包；

3. 3 种不同认证类型的用户终端同时访问 HTTP 业务；

4. 用户下线。

1. 预期结果:,步骤 2 中，3 台用户终端均能成功接入并通过认证。

2. 步骤 3 中，3 台 WLAN 用户终端均能成功使用 HTTP 业务。

3. SIM 以及 PEAP 认证的流程符合《中国移动无线局域网（WLAN）用户接入流程技术规范（SIMPEAP）》要求。

1. 备注：,需重点验证 SIM 及 PEAP 认证接入流程过程中，AC 按照用户认证、DHCP 服务器完成 IP 地址分配、AC 开始对用户计费的顺序进行；

2. 当用户下线时，AC 需与 RADIUS 服务器交互上报用户此次连接记录:以本次连接中 AC 开始计费时间为本次连接开始时间，以 AC 下线时间为本次用户下线时间。

7.1.2.2. AC 支持为不同的 SSID 提供不同的业务控制

项目:,不同 SSID 混合接入能力,分项目:,AC 支持为不同的 SSID 提供不同的业务控制

用例编号:,7.1.2.2,版本:,2.0.0

参考文档:,无,参考组网:,无

重要性:,基本要求,优先级:,A

测试目的:,检验 AC 为不同的 SSID 提供不同的业务控制的支持能力

1. 预置条件:,用户已获取了密码，并开通了相应的业务；

2. 已经正确安装网卡；

3. WLAN 用户申请 IP 地址正常；

4. WLAN 接入系统 WEB 认证功能配置正确。

1. 测试步骤:,AP 上配置四个 SSID，CMCC1、CMCC2、CMCC3、CMCC4；

2. AC 对 CMCC1 设置端口限制，限制访问如 3076、5200、6200 三个端口；

3. AC 对 CMCC2 设置带宽控制，设置上下行平均速率都为 512K；

4. AC 对 CMCC3 设置网页黑名单限制，设置某一网页地址为黑名单限制地址；

5. AC 对 CMCC4 设置免认证功能；

6. WLANUE 连接 CMCC1，通过认证后，访问如 3076、5200、6200 三个端口，然后访问 WWW 服务器；

7. WLANUE 连接 CMCC2，通过认证后，从 FTP 服务器下载、上传文件；

8. WLANUE 连接 CMCC3，通过认证后，访问设置为黑名单的网页地址；

9. WLANUE 连接 CMCC4，访问 WWW 服务器。

1. 预期结果:,步骤 6 中终端无法访问三个受限端口，终端正常访问 WWW 服务器。

2. 步骤 7 中终端的上下行平均速率是与所设置的平均速率一致（误差<5%），测试至少观察一分钟以上。

3. 步骤 8 中终端无法访问设置为黑名单的网页地址。

4. 步骤 9 中终端无需进行认证，正常访问 WWW 服务器。

1. 备注：,此测试项属于中国移动集团客户 WLAN 业务测试项。

7.1.2.3. AC 支持认证权限控制

项目:,不同 SSID 混合接入能力,分项目:,AC 支持认证权限控制

用例编号:,7.1.2.3,版本:,2.0.0

参考文档:,无,参考组网:,参见预置条件

重要性:,基本要求,优先级:,A

测试目的:,检验 AC 对认证权限控制的支持能力

预置条件:,参考组网：

1. 用户已获取了密码，并开通了相应的业务；

2. 已经正确安装网卡；

3. WLAN 用户申请 IP 地址正常；

4. WLAN 接入系统 WEB 认证功能配置正确。

1. 测试步骤:,配置帐号 1 为 CMCC-Starbucks 集团客户帐号，帐号 2 为普通 CMCC 帐号；

2. 配置 AP1 的 SSID 为 CMCC-Starbucks，AP2 的 SSID 为 CMCC；

3. WLAN 用户接入 AP1；

4. WLAN 用户在 Portal 页面上填写帐号 1 及密码，点击登陆；

5. WLAN 用户在 Portal 页面上填写帐号 2 及密码，点击登陆；

6. WLAN 用户接入 AP2；

7. WLAN 用户在 Portal 页面上填写帐号 1 及密码，点击登陆；

8. WLAN 用户在 Portal 页面上填写帐号 2 及密码，点击登陆。

1. 预期结果:,步骤 4 中用户登陆成功。

2. 步骤 5 中用户登陆失败。

3. 步骤 7 中用户登陆失败。

4. 步骤 8 中用户登陆成功。

1. 备注：,此测试项属于中国移动集团客户 WLAN 业务测试项。

7.1.2.4. AC 支持特殊场景下的认证权限控制

项目:,不同 SSID 混合接入能力,分项目:,AC 支持特殊场景下的认证权限控制

用例编号:,7.1.2.4,版本:,2.0.0

参考文档:,无,参考组网:,参见预置条件

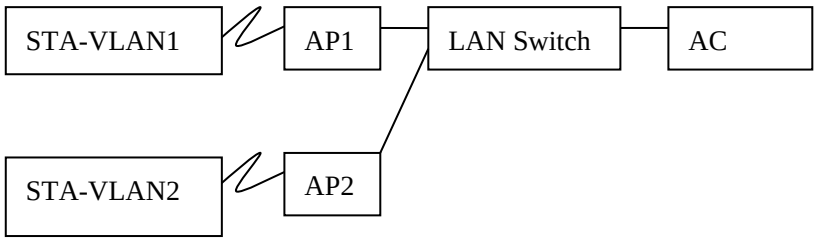
重要性:,基本要求,优先级:,A

1. 测试目的:,检验 AC 对特殊场景下认证权限控制的支持能力；

2. 在认证过程中发生 SSID 切换的认证权限控制支持能力；

3. 完成认证后发生 SSID 切换的认证权限控制支持能力。

预置条件:,参考组网：



1. 用户已获取了密码，并开通了相应的业务；

2. 已经正确安装网卡；

3. WLAN 用户申请 IP 地址正常；

4. WLAN 接入系统 WEB 认证功能配置正确。

1. 测试步骤:,配置帐号 1 为 CMCC-Starbucks 集团客户帐号，帐号 2 为普通 CMCC 帐号；

2. 配置 AP1 的 SSID 为 CMCC-Starbucks，AP2 的 SSID 为 CMCC；

3. WLAN 用户接入 AP1 并访问 WWW 服务器；

4. WLAN 用户在 Portal 页面弹出后，保留 Portal 页面，移动并接入到 AP2；

5. 在 Portal 页面上填写帐号 1 及密码，点击登陆；

6. 在 Portal 页面上填写帐号 2 及密码，点击登陆；

7. WLAN 用户访问 WWW 服务器；

8. WLAN 用户在 Portal 页面上填写帐号 2 及密码，点击登陆；

9. 用户下线；

10. WLAN 用户接入 AP1 并访问 WWW 服务器；

11. WLAN 用户在 Portal 页面上填写帐号 1 及密码，点击登陆；

12. WLAN 用户移动并接入到 AP2，访问 WWW 服务器。

1. 预期结果:,步骤 5 中用户登陆失败。

2. 步骤 6 中用户登陆失败。

3. 步骤 7 中用户被强制到 CMCCPortal 页面重新登陆。

4. 步骤 8 中用户登陆成功。

5. 步骤 11 中用户登陆成功。

6. 步骤 12 中用户无法访问 WWW 服务器，被强制到 CMCCPortal 页面重新登陆。

1. 备注：,此测试项属于中国移动集团客户 WLAN 业务测试项。

7.1.2.5. 不同 SSID 可配置开启/取消空闲时长下线的功能

项目:,不同 SSID 混合接入能力,分项目:,不同 SSID 可配置开启/取消空闲时长下线的功能

用例编号:,7.1.2.5,版本:,2.0.0

参考文档:,无,参考组网:,参见预置条件

重要性:,基本要求,优先级:,A

1. 测试目的:,检验 AC 对特殊场景下认证权限控制的支持能力；

2. 检验 AC 在同一个 AP 下的同一射频口下，不同 SSID 可以配置不同的空闲下线策略。

预置条件:,参考组网：

1. 用户已获取了密码，并开通了相应的业务；

2. 已经正确安装网卡；

3. 认证服务器配置正常；

4. WLAN 接入系统认证功能配置正确；

5. 配置交换机端口镜像，PC 可以抓取 AC 出方向的报文。

1. 测试步骤:,配置两个无线服务模板（SSID）CMCC1 和 CMCC2，CMCC1 使用 EAP-SIM 认证方式，CMCC2 使用 Portal 认证方式，两个服务均绑定到同一个 AP 的同一个射频口；

2. 开启 CMCC1 和 CMCC2 的空闲下线功能，CMCC1 的空闲时间为 3 分钟，流量阈值为 50K，CMCC2 的空闲时间为 5 分钟，流量阈值为 30K；

3. STA1 关联到 CMCC1，STA2 关联到 CMCC2，使用各自账号登陆上线，可以 ping 通 PC；

4. STA1 和 STA2 不进行任何操作，PC 抓取 AC 出方向报文；

5. 关闭 CMCC1 的空闲下线功能，再进行步骤 3，4 的测试；

6. 关闭 CMCC2 的空闲下线功能，开启 CMCC1 的空闲下线功能，再进行步骤 3，4 的测试。

1. 预期结果:,步骤 4 中，PC 可以抓取到 AC 向 radius 服务器发送 STA1 和 STA2 的用户计费停止报文。

2. 步骤 5 中，PC 可以抓取到 AC 向 radius 服务器发送 STA2 的用户计费停止报文，STA1 正常在线，可以 ping 通网关。

3. 步骤 6 中，PC 可以抓取到 AC 向 radius 服务器发送 STA1 的用户计费停止报文，STA2 正常在线，可以 ping 通网关。

1. 备注：,测试中需确保两个 ssid 配置在同一个射频口上。

7.1.2.6. 不同安全支持能力终端的混合接入支持（同一 SSID）

项目:,不同 SSID 混合接入能力,分项目:,不同安全支持能力终端的混合接入支持(同一 SSID)

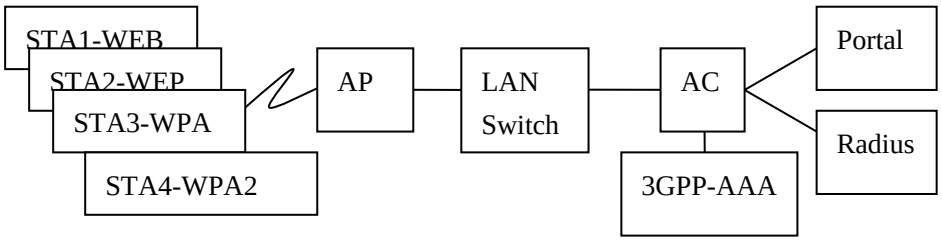
用例编号:,7.1.2.6,版本:,2.0.0

参考文档:,无,参考组网:,参见预置条件

重要性:,基本要求,优先级:,A

测试目的:,检验 WLAN 接入系统支持不同加密能力类型（包括不加密、静态 WEP 加密、WPA 加密、WPA2 加密）WLAN 用户终端的混合接入

预置条件:,参考组网：



1. WLAN 用户终端配置正确；

2. WLAN 接入系统配置正确；

3. 不同类型用户认证服务器配置正确并连接正确；

4. 相应的接入认证客户端软件成功安装；

5. 各系统正常运行。

1. 测试步骤:,4 台终端配置相同的 SSID 为“CMCC”；

2. 配置 4 台 WLAN 接入终端,分别采用 WEB（不加密）、静态 WEP 加密、PEAP-MSCHAPv2（WPA 加密）、PEAP-MSCHAPv2（WPA2 加密）的接入认证方式；

3. 依次接入这 4 种不同认证类型的用户终端；

4. 4 种不同认证类型的用户终端使用 HTTP 业务。

1. 预期结果:,步骤 3 中，4 台 WLAN 用户终端均能成功接入到 WLAN 接入网络中。

2. 步骤 4 中，4 台 WLAN 用户终端均能成功使用 HTTP 业务。

3. 步骤 4 中，通过抓包确认 4 台终端分别采用不同的加密方式。

1. 备注：,网卡应选取通过 wi-fiWPA 测试的第三方网卡；

2. 观察不同客户端软件的现象；

3. WEB 接入方式需考察 WEBPortal 认证，其他三种方式无需考察 Portal 认证。

7.1.2.7. 不同安全支持能力终端的混合接入支持（不同 SSID）

项目:,不同 SSID 混合接入能力,分项目:,不同安全支持能力终端的混合接入支持(不同 SSID)

用例编号:,7.1.2.7,版本:,2.0.0

参考文档:,无,参考组网:,参见预置条件

重要性:,基本要求,优先级:,A

测试目的:,检验 WLAN 接入系统支持不同加密能力类型（包括不加密、静态 WEP 加密、WPA 加密、WPA2 加密）WLAN 用户终端的混合接入

预置条件:,参考组网：

1. WLAN 用户终端配置正确；

2. WLAN 接入系统配置正确；

3. 不同类型用户认证服务器配置正确并连接正确；

4. 相应的接入认证客户端软件成功安装；

5. 各系统正常运行。

1. 测试步骤:,4 台终端配置不同的 SSID（如“WEB”，“WEP”，“WPA”，“WPA2”）；

2. 配置 4 台 WLAN 接入终端，分别采用 WEB（不加密）、静态 WEP 加密、PEAP-MSCHAPv2（WPATKIP 加密）、PEAP-MSCHAPv2（WPA2AES 加密）的接入认证方式；

3. 依次接入这 4 种不同认证类型的用户终端；

4. 4 种不同认证类型的用户终端使用 HTTP 业务。

1. 预期结果:,步骤 3 中，4 台 WLAN 用户终端均能成功接入到 WLAN 接入网络中。

2. 步骤 4 中，4 台 WLAN 用户终端均能成功使用 HTTP 业务。

3. 步骤 4 中，通过抓包确认 4 台终端分别采用不同的加密方式。

1. 备注：,网卡应选取通过 wi-fiWPA 测试的第三方网卡；

2. （观察不同客户端软件的现象）；

3. WEB 接入方式需考察 WEBPortal 认证，其他三种方式无需考察 Portal 认证。

7.1.3. 客户端及其他认证（PPPOE）认证

7.1.3.1. AC 支持随 e 行客户端接入的能力

项目:,客户端及其他认证（PPPOE）认证,分项目:,AC 支持随 e 行客户端接入的能力

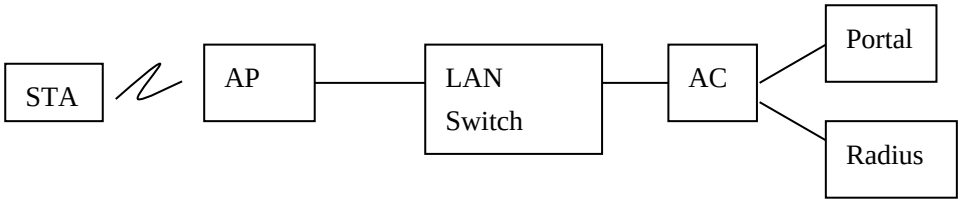
用例编号:,7.1.3.1,版本:,2.0.0

参考文档:,无,参考组网：,参见预置条件

重要性:,基本要求,优先级:,A

测试目的:,检验 AC 对随 e 行客户端接入认证的支持能力

预置条件:,参考组网：



1. “随 e 行”用户已获取了密码，并开通了业务；

2. 已经正确安装网卡，并且已经配置了网卡和 AP 之间的静态共享密钥；

3. AC 和 RADIUS 进行相关配置，配置互通的 IP 地址和 Key 值；

4. WLAN 用户申请 IP 地址正常；

5. WEB 认证功能正确配置；

6. 认证点、RADIUS 用户认证服务器正确配置完毕；

7. 安装并启动“随 e 行”客户端软件。

1. 测试步骤:,将待测 AP 的 SSID 配置为“CMCC”；

2. 点击“随 e 行”客户端软件的连接按钮，启动用户认证流程；

3. 用户输入正确的帐号和密码后进行认证；

4. 认证成功后，用户终端访问 WWW 服务器。

1. 预期结果:,步骤 3 中 WLAN 用户通过“随 e 行”客户端认证成功。

2. 步骤 4 中用户认证成功后可以访问 WWW 服务器。

备注：,1·测试终端原则上要求涵盖 PC 和手机，其中手机应该包括当前各类主流操作系统的典型机型；

2·AC 向“随 e 行”客户端推送界面要求如下：

《AC 控制器页面推送规范》

1. 跳转页面

跳转页面必须采用如下方法进行跳转；

2. 方法：通过 HTTP 协议状态码为 302 的重定向操作进行跳转的方式

a) 内容定义

该方式必须符合 HTTP 协议的要求，即状态码为 302 的 HTTP 协议包的 Location 头域中存放“完整的重定向页面地址”。如：

Location:221.176.1.140?wlanacname=1016.0010.100.00&wlanuserip=117.128.216.199&ssid=CMCC；

b) WLAN 客户端与 AC 交互过程

采用该方法跳转时，WLAN 客户端将不会分析页面内容，直接根据“完整的重定向页面地址”访问下一跳页面。

7.1.3.2.　AC 支持国际漫游客户端接入的能力

项目:,客户端及其他认证（PPPOE）认证,分项目:,AC 支持国际漫游客户端接入的能力

用例编号:,7.1.3.2,版本:,2.0.0

参考文档:,《中国移动 WLAN 国际漫游业务总体技术要求》,参考组网：,参见预置条件

重要性:,基本要求,优先级:,A

测试目的:,检验 AC 对国际漫游客户端 iPass 接入认证的支持能力，保证国际漫游用户的正常认证

预置条件:,参考组网：

1. 国际漫游用户已在归属地开通业务，并取得了用户名和密码；

2. 已经正确安装无线网卡，申请 IP 地址正常；

3. 在 WLANUE 上安装 iPass 客户端；

4. 网络环境下更新客户端的地址簿。

1. 测试步骤:,在 WLAN 热点找到 SSID 为 CMCC 的无线信号；

2. 打开 iPass 客户端软件；

3. 用户在 SSID 栏填写“CMCC”；

4. 点击“下一步”；

5. 客户端会要求用户输入用户名和密码；

6. 用户输入正确的认证信息；

7. 客户端对用户信息进行认证；

8. 认证成功后，用户访问互联网。

1. 预期结果:,步骤 7 中用户通过 iPass 客户端认证。

2. 步骤 8 中用户成功访问 WWW 网页。

1. 备注:,按照 WISPr 协议的规定，为支持国际漫游客户端的接入，当 AC 实现强制 PORTAL 功能时，要求在原有代码的基础上，增加 Proxy 方式的代码供客户端跳转，并按照《中国移动 WLAN 业务 PORTAL 协议规范》传递强制 PORTAL 功能相关参数。

接口的详细参数描述如下表所示：

AC 与一级 Portal 接口属性

属性名,字段格式

MessageType,<MessageType>

110

</MessageType>

Response,<ResponseCode>

{ResponseCodedata}

</ResponseCode>

NextURL,<NextURL>

<sitespecificURL>

</NextURL>

其中 ResponseCode 的意义说明如下表所示：

AC 与一级 Portal 接口响应码

ResponseCode,说明

200,Proxydetection/repeatoperation

例如：

<?xmlversion="1.0"encoding="UTF-8"?>

<WISPAccessGatewayParam

xmlns:xsi="/">

<Proxy>

<MessageType>110</MessageType>

<NextURL>192.168.10.132:7080?wlanacname=020.010.100.00&wlanuserip=192.168.2.12

</NextURL>

<ResponseCode>200</ResponseCode>

</Proxy>

</WISPAccessGatewayParam>

7.1.3.3. AC 支持 PPPoE 认证的能力

项目:,客户端及其他认证（PPPOE）认证,分项目:,AC 支持 PPPoE 认证的能力

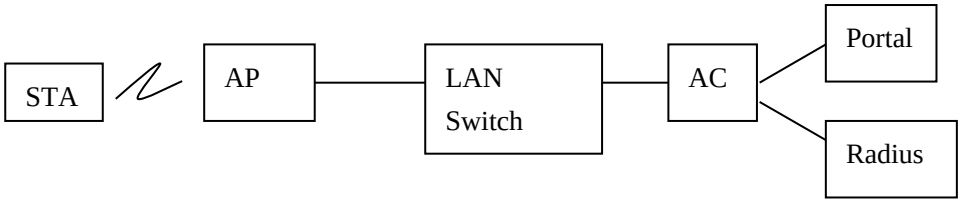
用例编号:,7.1.3.3,版本:,2.0.0

参考文档:,无,参考组网:,参见预置条件

重要性:,基本要求,优先级:,A

测试目的:,检验 AC 对 PPPoE 认证的支持能力

预置条件:,参考组网：



1. 用户已获取了密码，并开通了相应的业务；

2. 已经正确安装网卡；

3. WLAN 用户申请 IP 地址正常；

4． WLAN 接入系统 WEB 认证功能配置正确；

5． AC 开启 PPPoE 认证功能；

6． 测试步骤:,用户通过 PPPoE 拨号软件登陆，并访问 WWW 网页后退出登陆；

7． 用户通过 Web 方式认证，并访问 WWW 网页。

1． 预期结果:,步骤 1 中用户认证成功，用户 IP 地址在认证成功后分配，用户成功访问 WWW 网页。

2． 步骤 2 中用户认证成功，并成功访问 WWW 网页。

1． 备注：,AC 需同时支持两种认证方式，PPPoE 认证和 Web 认证。

7.2. 计费功能测试

7.2.1. 预付费测试

项目:,计费功能测试,分项目:,预付费测试

用例编号:,7.2.1,版本:,2.0.0

参考文档:,无,参考组网:,参见预置条件

重要性:,基本要求,优先级:,A

测试目的:,测试后台的 Radius 系统能支持预付费业务

预置条件:,参考组网：

1． 用户已获取了密码，并开通了相应的业务；

2． 已经正确安装网卡；

3． WLAN 用户申请 IP 地址正常；

4． AC 上 WEB 和无感知认证功能配置正确，采用外置 Radius/AAA 认证和计费；

5． Radius 计费服务器上设置用户的通话时间为 3 分钟。

1． 测试步骤:,终端用户连接 WLAN 网络；

2． 终端用户分别进行 WEB 认证和无感知认证接入 WLAN 网络；

3． 终端用户一直访问 Internet；

4． 3 分钟后，Radius 服务器通知 WLAN 接入系统切断用户连接，用户不能访问 Internet；

5． 重复步骤 2。

1． 预期结果:,在步骤 2 中，终端用户通过认证。

2． 在步骤 3 中，终端用户可以访问 Internet。

3． 在步骤 4 中，3 分钟后，终端用户预付费金额用完，用户应用被切断。

4． 步骤 5 中，用户无法再成功通过认证，也无法访问 Internet。

1． 备注：,要求 AC 支持周期性计费信息上报功能。

7.2.2. 流量计费测试