

团 体 标 准

T/WAPIA 041.1—2021

关键信息基础设施无线局域网测试方法 第 1 部分：通用部分

WLAN test method of critical information infrastructure -
Part 1: General part

2021-11-05 发布

2021-11-05 实施

中关村无线网络安全产业联盟 发布

版权声明

本文件版权归中关村无线网络安全产业联盟（WAPI产业联盟）©所有。

本文件以电子文档形式面向公众公开。本声明在此授权所有组织或者个人对本文件进行使用和复制。任何组织或者个人对本文件的修改、翻译、摘编、汇编、销售行为，应事先获得WAPI产业联盟书面授权，否则视为侵权。

联系WAPI产业联盟标准化部（lmbz@wapia.org）可获取本文件授权相关信息。

WAPI Alliance

全国团体标准信息平台

WAPI Alliance

目 次

版权声明	I
前言	V
引言	VII
1 范围	1
2 规范性引用文件	1
3 术语和定义	2
4 缩略语	2
5 概述	3
6 安全协议测试	3
6.1 SSID 配置	3
6.2 WAPI 证书安装	3
6.3 WAPI-PSK 接入	3
6.4 WAPI-Cert 接入	3
6.5 加密传输	4
6.6 密钥更新	4
6.7 否定非法证书	4
6.8 证书选择	4
7 物理接口测试	4
7.1 网络侧物理接口	4
7.2 用户侧物理接口	4
8 运行环境测试	5
8.1 物理环境	5
8.2 电磁兼容性	5
9 功能测试	6
9.1 无线接入点	6
9.2 接入点控制器	11
9.3 鉴别服务器	15
9.4 证书签发服务器	16
9.5 终端	17
10 性能测试	18
10.1 无线接入点	18
10.2 接入点控制器	19
10.3 鉴别服务器	19
10.4 证书签发服务器	20
10.5 终端	20
附录 A (资料性) 技术要求与测试方法对照表	21
A.1 无线接入点测试	21
A.2 接入点控制器测试	23
A.3 鉴别服务器测试	24
A.4 证书签发服务器测试	25

A.5 终端测试 26

WAPI Alliance

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规则起草。

本文件是 T/WAPIA 041《关键信息基础设施无线局域网测试方法》的第1部分。T/WAPIA 041 已经发布了以下部分：

— 第1部分：通用部分。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中关村无线网络安全产业联盟与工业和信息化部宽带无线 IP 标准工作组联合提出。

本文件由无线网络安全标准化委员会归口。

本文件起草单位：中关村无线网络安全产业联盟、西安西电捷通无线网络通信股份有限公司、无线网络安全技术国家工程实验室、中国电力科学研究院有限公司、南方电网科学研究院有限责任公司、广州广电计量检测股份有限公司、江苏省电子信息产品质量监督检验研究院（江苏省信息安全测评中心）、北京数字认证股份有限公司、深圳市信锐网科技有限公司、北京华信傲天技术股份有限公司、新华三技术有限公司、国家无线电监测中心检测中心、国家信息技术安全研究中心、深圳市瑞科慧联科技有限公司、深圳智开科技有限公司、迈普通信技术股份有限公司、巷子科技（北京）有限公司、北京三凯威科技有限公司、天津市无线电监测站、WAPI 产业联盟测试实验室、工业和信息化部宽带无线 IP 标准工作组。

本文件主要起草人：潘琪、王立华、简练、张国强、黄振海、张璐璐、范小伟、方帅、严敏辉、肖笃亮、侯鹏亮、卢杰、刘高锦、禹凯、郑骊、尹玉昂、陈晓龙、匡晓云、陈立明、索思亮、杨韬、李楠、蓝海昌、祝张睿、王玉斐、李楠、张海涛、袁成、王太军、葛珊、赵天旭、谭鑫、任成龙、韩志强、江涛、张永才、王勇、姜敏、高德龙、张变玲、周涛、刘婷、周园、匡俊华、王庆、杜宾、肖非。

WAPI Alliance

引 言

随着网络安全法、密码法和网络安全等级保护等相关法律法规和国家标准的发布实施，显著激发了关键信息基础设施中采用 WAPI 技术和产品保障无线网络安全的需求，WAPI 技术和产品得到了广泛应用。在相关行业的应用，尤其是针对关键信息基础设施应用的采购和部署，涉及到无线局域网（WLAN）部分，目前缺乏明确和统一的指导。无线网络安全标准化委员会组织开展了 T/WAPIA 040 系列团体标准及其对应测试标准 T/WAPIA 041《关键信息基础设施无线局域网测试方法》的制定工作。

T/WAPIA 041 旨在制定应用于关键信息基础设施的无线局域网系统及设备的测试方法，给联盟成员单位、业内厂商以及相关行业部门、机构等提供准确、完整的测试规范，确保产品设计、生产和采购、部署等环节的合规性和一致性。T/WAPIA 041 拟由以下几部分构成。

- 第 1 部分，通用部分。目的在于确立关键信息基础设施及相关环境中应用无线局域网的通用测试方法。
- 第 2 部分，电力行业扩展部分。目的在于确立电力行业及相关环境中应用无线局域网的特殊测试方法。

T/WAPIA 041 将来可能会随着 T/WAPIA 040 的修订和增补，增加其他领域的扩展测试方法。

WAPI Alliance

关键信息基础设施无线局域网测试方法

第1部分：通用部分

1 范围

本文件规定了在关键信息基础设施中应用无线局域网的通用测试方法。

本文件适用于指导相关行业开展无线局域网设备采购、生产和无线局域网网络建设过程中的各类测试。具体包括：

- a) 安全协议测试；
- b) 物理接口测试；
- c) 运行环境测试；
- d) 功能测试；
- e) 性能测试。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

- GB/T 2423.1—2008 电工电子产品环境试验 第2部分：试验方法 试验A：低温
- GB/T 2423.2—2008 电工电子产品环境试验 第2部分：试验方法 试验B：高温
- GB/T 2423.3—2016 环境试验 第2部分：试验方法 试验Cab：恒定湿热试验
- GB/T 2423.5—2019 环境试验 第2部分：试验方法 试验Ea和导则：冲击
- GB/T 2423.7—2018 环境试验 第2部分：试验方法 试验Ec：粗率操作造成的冲击（主要用于设备型样品）
- GB/T 2423.10—2019 环境试验 第2部分：试验方法 试验Fc：振动（正弦）
- GB/T 2423.17—2008 电工电子产品环境试验 第2部分：试验方法 试验Ka：盐雾
- GB/T 4208—2017 外壳防护等级（IP代码）
- GB/T 5080.7—1986 设备可靠性试验 恒定失效率假设下的失效率与平均无故障时间的验证试验方案
- GB/T 9254—2008 信息技术设备的无线电骚扰限值和测量方法
- GB 15629.11（所有部分） 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范
- GB/T 17626.2—2018 电磁兼容 试验和测量技术 静电放电抗扰度试验
- GB/T 17626.3—2016 电磁兼容 试验和测量技术 射频电磁场辐射抗扰度试验
- GB/T 17626.4—2018 电磁兼容 试验和测量技术 电快速瞬变脉冲群抗扰度试验
- GB/T 17626.5—2019 电磁兼容 试验和测量技术 浪涌（冲击）抗扰度试验
- GB/T 17626.6—2017 电磁兼容 试验和测量技术 射频场感应的传导骚扰抗扰度试验
- GB/T 17626.8—2006 电磁兼容 试验和测量技术 工频磁场抗扰度试验
- GB/T 17626.11—2008 电磁兼容 试验和测量技术 电压暂降、短时中断和电压变化抗扰度试验
- GB/T 21671—2018 基于以太网技术的局域网（LAN）系统验收测试方法
- GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求
- GB/T 32420—2015 无线局域网测试规范
- YD/T 1098—2009 路由器设备测试方法 边缘路由器

T/WAPIA 041.1—2021

YD/T 1141—2007 以太网交换机测试方法

YD/T 1453—2014 IPv6网络设备测试方法 边缘路由器

T/WAPIA 037.2—2021 无线局域网测试 第2部分：设备测试规范

T/WAPIA 040.1—2020 关键信息基础设施无线局域网技术指标 第1部分：通用要求

3 术语和定义

GB/T 32420—2015界定的以及下列术语和定义适用于本文件。

3.1

证书签发服务器 certificate issue server

对无线局域网终端、无线接入点和鉴别服务器提供证书签发管理服务的设备，该管理服务包括证书签发、证书吊销列表签发、证书吊销、证书查询和证书更新等。

3.2

WAPI预共享密钥方式 WAPI pre-shared key mode

通过预共享密钥完成单播密钥协商和组播密钥通告，实现身份鉴别、密钥协商和接入控制的WAPI安全机制。

3.3

WAPI证书方式 WAPI certificate mode

通过证书完成证书鉴别、单播密钥协商和组播密钥通告，实现身份鉴别、密钥协商和接入控制的WAPI安全机制。

3.4

终端 terminal

包含符合GB 15629.11系列媒体访问控制和物理层规范的无线局域网STA功能模块的设备。

[来源：T/WAPIA 040.1—2020]

4 缩略语

下列缩略语适用于本文件。

AC	接入点控制器 (AP controller)
ACL	访问控制列表 (access control list)
AP	无线接入点 (access point)
AS	鉴别服务器 (authentication server)
CIS	证书签发服务器 (certificate issue server)
CRL	证书吊销列表 (certificate revocation list)
DHCP	动态主机配置协议 (dynamic host configuration protocol)
DoS	拒绝服务 (denial of service)
IP	互联网协议 (Internet protocol)
IPv4	第4版互联网协议 (Internet protocol version 4)
IPv6	第6版互联网协议 (Internet protocol version 6)
LAN	局域网 (local area network)
MAC	媒体访问控制 (medium access control)
MTBF	平均失效间隔时间 (mean time between failure)
NAT	网络地址转换 (network address translation)
NTP	网络时间协议 (network time protocol)
PING	互联网分组探索 (packet internet groper)

PPPoE	以太网上的点对点协议 (point-to-point protocol over ethernet)
QoS	服务质量 (quality of service)
SLAAC	无状态地址自动配置 (stateless address auto configuration)
SSID	服务集标识 (service set identifier)
STA	站 (点) (station)
STP	生成树协议 (spanning tree protocol)
TCP	传输控制协议 (transmission control protocol)
UDP	用户数据报协议 (user datagram protocol)
URL	统一资源定位符 (uniform resource locator)
VLAN	虚拟局域网 (virtual local area network)
WAPI	无线局域网鉴别与保密基础结构 (wireless LAN authentication and privacy infrastructure)
WAPI-Cert	WAPI 证书方式 (WAPI certificate mode)
WAPI-PSK	WAPI 预共享密钥方式 (WAPI pre-shared key mode)
WLAN	无线局域网 (wireless local area network)

5 概述

本文件所涉及的无线局域网网络系统由以下五种类型的设备组成：AP、AC、AS、CIS和终端。这五种类型设备的无线及空口等安全功能应符合GB 15629.11（所有部分）的规定，详细技术要求应符合T/WAPIA 040.1的规定，技术指标与测试项目对应关系见附录A。

6 安全协议测试

6.1 SSID 配置

无线接入点SSID配置的测试步骤和判定准则应符合GB/T 32420—2015中7.2.3.1的相关规定，并参照团体标准T/WAPIA 037.2—2021中7.3.1的相关内容。

终端SSID配置的测试步骤和判定准则应符合GB/T 32420—2015中7.1.3.1的相关规定，并参照团体标准T/WAPIA 037.2—2021中6.3.1的相关内容。

6.2 WAPI 证书安装

无线接入点WAPI证书安装的测试步骤和判定准则应符合GB/T 32420—2015中7.2.3.8.2的相关规定，并参照团体标准T/WAPIA 037.2—2021中7.3.8.2的相关内容。

终端WAPI证书安装的测试步骤和判定准则应符合GB/T 32420—2015中7.1.3.8.2的相关规定，并参照团体标准T/WAPIA 037.2—2021中6.3.8.2的相关内容。

6.3 WAPI-PSK 接入

无线接入点WAPI-PSK接入的测试步骤和判定准则应符合GB/T 32420—2015中7.2.3.8.1的相关规定，并参照团体标准T/WAPIA 037.2—2021中7.3.8.1的相关内容。

终端WAPI-PSK接入的测试步骤和判定准则应符合GB/T 32420—2015中7.1.3.8.1的相关规定，并参照团体标准T/WAPIA 037.2—2021中6.3.8.1的相关内容。

6.4 WAPI-Cert 接入

T/WAPIA 041.1—2021

无线接入点WAPI-Cert接入的测试步骤和判定准则应符合GB/T 32420—2015中7.2.3.8.3的相关规定，并参照团体标准T/WAPIA 037.2—2021中7.3.8.3的相关内容。

终端WAPI-Cert接入的测试步骤和判定准则应符合GB/T 32420—2015中7.1.3.8.4的相关规定，并参照团体标准T/WAPIA 037.2—2021中6.3.8.4的相关内容。

鉴别服务器WAPI-Cert接入的测试步骤和判定准则应符合GB/T 32420—2015中7.3.3.2的相关规定，并参照团体标准T/WAPIA 037.2—2021中8.3.2的相关内容。

6.5 加密传输

无线接入点加密传输的测试步骤和判定准则应符合GB/T 32420—2015中7.2.3.8.4的相关规定，并参照团体标准T/WAPIA 037.2—2021中7.3.8.4的相关内容。

终端加密传输的测试步骤和判定准则应符合GB/T 32420—2015中7.1.3.8.5的相关规定，并参照团体标准T/WAPIA 037.2—2021中6.3.8.5的相关内容。

6.6 密钥更新

无线接入点密钥更新的测试步骤和判定准则应符合GB/T 32420—2015中7.2.3.8.5的相关规定，并参照团体标准T/WAPIA 037.2—2021中7.3.8.5的相关内容。

终端密钥更新的测试步骤和判定准则应符合GB/T 32420—2015中7.1.3.8.6的相关规定，并参照团体标准T/WAPIA 037.2—2021中6.3.8.6的相关内容。

6.7 否定非法证书

无线接入点否定非法证书的测试步骤和判定准则应符合GB/T 32420—2015中7.2.4.6的相关规定，并参照团体标准T/WAPIA 037.2—2021中7.4.6的相关内容。

终端的否定非法证书的测试步骤和判定准则应符合GB/T 32420—2015中7.1.4.2的相关规定，并参照团体标准T/WAPIA 037.2—2021中6.4.2的相关内容。

6.8 证书选择

终端证书选择的测试步骤和判定准则应符合GB/T 32420—2015中7.1.3.8.3的相关规定，并参照团体标准T/WAPIA 037.2—2021中6.3.8.3的相关内容。

7 物理接口测试

7.1 网络侧物理接口

测试步骤和判定准则应符合GB/T 21671—2018中6.2.2.1的相关规定。

7.2 用户侧物理接口

7.2.1 10/100/1000 Base-T 以太网接口

测试步骤和判定准则应符合GB/T 21671—2018中6.2.2.1的相关规定。

7.2.2 串口

串口测试步骤和判定准则如下。

a) 测试步骤：

- 1) 连接设备串口与计算机串口；
- 2) 设置波特率、奇偶校验位等；
- 3) 输入设备串口登录的用户名、密码。

b) 判定准则:

测试步骤3)中,应以测试步骤3)中的用户身份登录设备。

8 运行环境测试

8.1 物理环境

8.1.1 低温试验

测试步骤和判定准则应符合GB/T 2423.1—2008中第5章和第6章的相关规定。

8.1.2 高温试验

测试步骤和判定准则应符合GB/T 2423.2—2008中第5章和第6章的相关规定。

8.1.3 恒定湿热试验

测试步骤和判定准则应符合GB/T 2423.3—2016中第4章和第5章的相关规定。

8.1.4 冲击试验

测试步骤和判定准则应符合GB/T 2423.5—2019中第4~10章的相关规定。

8.1.5 跌落试验

测试步骤和判定准则应符合GB/T 2423.7—2018中第3~6章的相关规定。

8.1.6 振动试验

测试步骤和判定准则应符合GB/T 2423.10—2019中第4~11章的相关规定。

8.1.7 盐雾腐蚀

测试步骤和判定准则应符合GB/T 2423.17—2008中第4~8章的相关规定。

8.1.8 外壳防护试验

测试步骤和判定准则应符合GB/T 4208—2017中第12~15章的相关规定。

8.2 电磁兼容性

8.2.1 电源端传导骚扰

测试步骤和判定准则应符合GB/T 9254—2008中5.1和第9章的相关规定。

8.2.2 电信端口传导共模骚扰

测试步骤和判定准则应符合GB/T 9254—2008中5.2和第9章的相关规定。

8.2.3 辐射骚扰

测试步骤和判定准则应符合GB/T 9254—2008中第6章和第10章的相关规定。

8.2.4 静电放电抗扰度

测试步骤和判定准则应符合GB/T 17626.2—2018中第5章和第8章的相关规定。

8.2.5 射频电磁场辐射抗扰度

测试步骤和判定准则应符合GB/T 17626.3—2016中第5章、第7章和第8章的相关规定。

8.2.6 电快速瞬变脉冲群抗扰度

测试步骤和判定准则应符合GB/T 17626.4—2018中第5章、第7章和第8章的相关规定。

8.2.7 浪涌（冲击）抗扰度

测试步骤和判定准则应符合GB/T 17626.5—2016中第5章、第7章和第8章的相关规定。

8.2.8 射频场感应的射频传导骚扰抗扰度

测试步骤和判定准则应符合GB/T 17626.6—2017中第5章、第7章和第8章的相关规定。

8.2.9 工频磁场抗扰度

测试步骤和判定准则应符合GB/T 17626.8—2006中第5章、第7章和第8章的相关规定。

8.2.10 电压暂降、短时中断和电压变化抗扰度

测试步骤和判定准则应符合GB/T 17626.11—2008中第5章、第7章和第8章的相关规定。

9 功能测试

9.1 无线接入点

9.1.1 IPv4/IPv6 双栈协议支持

IPv4/IPv6双栈协议支持测试连接图见图1。

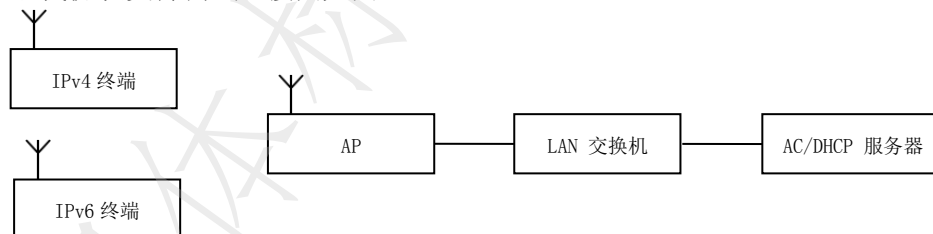


图1 IPv4/IPv6 双栈协议支持测试连接图

测试步骤和判定准则如下。

a) 测试步骤:

- 1) 搭建IPv4、IPv6双链路的无线网络，使用DHCP V4、IPv6 SLAAC地址分配模式；
- 2) 配置一个IPv4地址池Pool1和一个IPv6地址池Pool2；其中Pool1负责为VLAN100分配地址，配置IP网段为192.168.100.0/24，配置三层接口IP地址为192.168.100.1；Pool2负责为VLAN200分配地址，配置IPv6网段为2001::/24，配置三层接口IPv6地址为2001::1/24；
- 3) 配置两个明文WLAN服务，SSID分别为“IPv4”和“IPv6”，并同时在AP的空口上应用；将“IPv4”映射到VLAN100，“IPv6”映射到VLAN200；
- 4) IPv4终端、IPv6终端均配置为自动获取地址，并分别接入SSID“IPv4”和“IPv6”，浏览网页并查看终端所获得的IP地址。

b) 判定准则:

测试步骤4)中，IPv4终端、IPv6终端均应正常浏览网页，并分别获得192.168.100.0/24网段地址、2001::/24网段地址。

9.1.2 AC 发现方式

AC方发现方式测试连接图见图2。

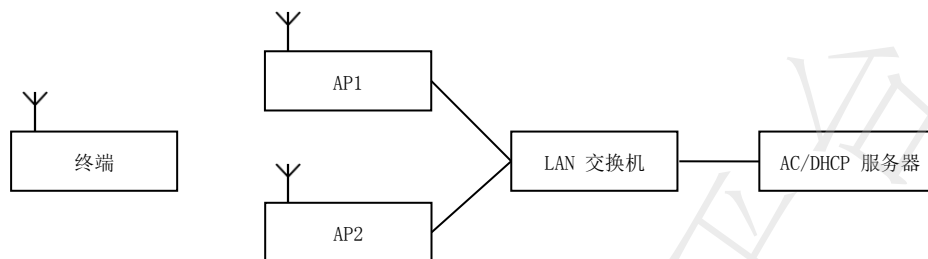


图2 AC发现方式测试连接图

测试步骤和判定准则如下。

a) 测试步骤：

- 1) AC与两台以上AP在同一二层网络内组网；
- 2) AP手动设置AC地址，查看AC对AP的管理状态，终端进行网页浏览；
- 3) 清除AP手动设置的AC地址，改为通过DHCP的43选项（厂商特定信息选项）设置AC地址，查看AC对AP的管理状态，终端进行网页浏览；
- 4) 改为通过DHCP的52选项（附加选项）设置AC地址，查看AC对AP的管理状态，终端进行网页浏览。

b) 判定准则：

测试步骤2)～4)中，AC应查看到AP的当前状态，终端应正常浏览网页。

9.1.3 业务转发方式

业务转发方式测试连接图见图2，测试步骤和判定准则如下。

a) 测试步骤：

- 1) AP经过二层交换机连接至AC，部署在同一个二层VLAN内，采用本地转发模式；配置WAPI-PSK接入方式，并进行终端浏览网页操作；
- 2) 在交换机设置端口镜像并抓包，查看受测终端的目的MAC地址；
- 3) 如AC支持集中转发模式，则设置为集中转发模式后，重复测试步骤2)；
- 4) 如AC支持集中转发模式，则设置为集中转发模式，配置NAT功能，并进行终端浏览网页操作；在AC侧端口镜像抓包；
- 5) 如AC支持集中转发模式且支持上行PPPoE拨号功能，则设置为集中转发模式，配置AC仅支持上行PPPoE拨号功能，并进行终端浏览网页操作；
- 6) 如AC支持集中转发模式且支持上行静态IP地址接入，则设置为集中转发模式，配置AC仅支持上行静态IP地址接入，并进行终端浏览网页操作；
- 7) 如AC支持集中转发模式且支持上行DHCP自动获取地址，则设置为集中转发模式，配置AC仅支持上行DHCP自动获取地址，并进行终端浏览网页操作。

b) 判定准则：

- 1) 测试步骤2)中，如目的MAC地址不是AC的MAC地址，且终端浏览网页正常，则判定为本地转发模式；
- 2) 测试步骤3)中，如目的MAC地址是AC的MAC地址，且终端浏览网页正常，则判定为集中转发模式；
- 3) 测试步骤4)中，终端应正常浏览网页；抓包数据应显示，终端MAC地址按照源NAT转化规则成功进行了地址转换；
- 4) 测试步骤5)～7)中，终端应正常浏览网页。

9.1.4 漫游切换

漫游切换测试连接图见图3。

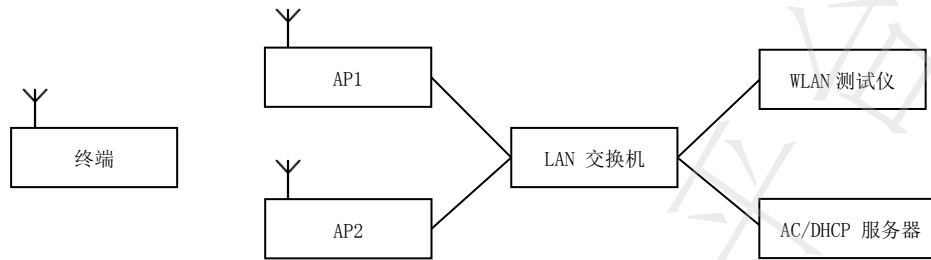


图3 漫游切换测试连接图

测试步骤和判定准则如下。

a) 测试步骤:

- 1) AP1和AP2部署在同一个二层网络内，并设置相同名称的SSID；AP1和AP2的部署间隔超过5米，并设置每台AP的传导发射功率为10 dBm；
- 2) 终端接入AP1并浏览网页，同时以正常步行速度向AP2移动；
- 3) 使用WLAN测试仪进行抓包分析。

b) 判定准则:

- 1) 测试步骤2)中，漫游期间网页浏览不应中断；
- 2) 测试步骤3)中，抓包数据应看到AP1侧的终端解除关联报文及AP2侧的终端关联报文。

9.1.5 功率控制

功率控制测试步骤和判定准则如下。

a) 测试步骤:

- 1) 设置无线接入点工作在人工设定的发射功率值模式（例如8 dBm），然后通过命令行查看发射功率；
- 2) 设置无线接入点工作在自动发射功率设置模式，然后通过命令行查看发射功率。

b) 判定准则:

- 1) 测试步骤1)中，查看到的发射功率值应与设置值相同；
- 2) 测试步骤2)中，查看到的发射功率值应与测试步骤1)中设置的值不同。

9.1.6 接入控制

9.1.6.1 测试连接

接入控制测试连接图见图4，其中终端数量应根据具体测试项目选择使用。

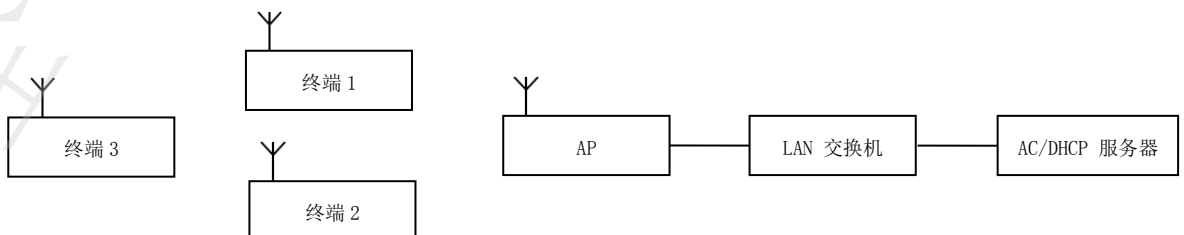


图4 接入控制测试连接图

9.1.6.2 简单接入控制

简单接入控制测试连接图见图4，测试步骤和判定准则如下。

- a) 测试步骤：
 - 1) AP/AC设置仅允许终端1对应的MAC地址进行接入，并使用终端1接入AP；
 - 2) 使用终端2和终端3接入AP。
- b) 判定准则：
 - 1) 测试步骤1)中，终端1应接入AP；
 - 2) 测试步骤2)中，终端2和终端3不应接入AP。

9.1.6.3 限制最大关联用户数

限制最大关联用户数测试连接图见图4，测试步骤和判定准则如下。

- a) 测试步骤：
 - 1) AP/AC设置基于SSID的最大关联用户数为2；
 - 2) 使用终端1、终端2接入AP；
 - 3) 使用终端3接入AP。
- b) 判定准则：
 - 1) 测试步骤1)中，查看设置的最大关联用户数应为2；
 - 2) 测试步骤2)中，终端1和终端2应接入AP；
 - 3) 测试步骤3)中，终端3不应接入AP。

9.1.6.4 多SSID能力

多SSID能力测试连接图见图4，测试步骤和判定准则如下。

- a) 测试步骤：
 - 1) AP/AC配置8个SSID，使用终端分别接入8个SSID；
 - 2) AP/AC设置SSID1、SSID3分别绑定不同的VLAN地址，两个终端分别接入这两个SSID，并对对方执行PING操作。
- b) 判定准则：
 - 1) 测试步骤1)中，应成功设置8个SSID，且终端应分别接入该8个SSID；
 - 2) 测试步骤2)中，PING结果显示两个终端不应连通。

9.1.7 用户隔离

用户隔离测试连接图见图4，测试步骤和判定准则如下。

- a) 测试步骤：
 - 1) AP/AC配置SSID，并设置该SSID绑定1个VLAN地址，两个终端分别接入AP；
 - 2) 查看AP/AC“二层隔离”默认设置；
 - 3) 打开“二层隔离”，两个终端对对方执行PING操作；
 - 4) 关闭“二层隔离”，两个终端对对方执行PING操作。
- b) 判定准则：
 - 1) 测试步骤2)中，“二层隔离”开关默认应为打开状态；
 - 2) 测试步骤3)中，PING结果显示两个终端不应连通；
 - 3) 测试步骤4)中，PING结果显示两个终端应连通。

9.1.8 VLAN 功能

WLAN功能测试连接图见图4，测试步骤和判定准则如下。

a) 测试步骤：

- 1) AP设置SSID1、SSID2分别绑定VLAN1、VLAN2；终端1、终端2分别接入SSID1、SSID2，在交换机侧设置端口镜像并抓包查看VLAN标记；
- 2) AP上行端口配置VLAN1通过，终端1、终端2分别浏览网页；
- 3) AP上行端口配置VLAN 端口汇聚功能，允许VLAN1、VLAN2通过，终端1、终端2分别浏览网页。

b) 判定准则：

- 1) 测试步骤1) 中，终端1和终端2的抓包数据中均应查看到正确的VLAN标记；
- 2) 测试步骤2) 中，终端1应正常浏览网页，终端2应无法浏览网页；
- 3) 测试步骤3) 中，终端1和终端2均应正常浏览网页。

9.1.9 强制 STA 下线

测试步骤和判定准则应符合GB/T 32420—2015中7.2.4.4的相关规定，并参照团体标准T/WAPIA 037.2—2021中7.4.4的相关内容。

9.1.10 QoS 支持

测试步骤和判定准则应符合GB/T 32420—2015中7.2.3.6的相关规定，并参照团体标准T/WAPIA 037.2—2021中7.3.6的相关内容。

9.1.11 信标间隔设置

测试步骤和判定准则应符合GB/T 32420—2015中7.2.3.4的相关规定，并参照团体标准T/WAPIA 037.2—2021中7.3.4的相关内容。

9.1.12 动态速率切换

测试步骤和判定准则应符合GB/T 32420—2015中7.2.4.2的相关规定，并参照团体标准T/WAPIA 037.2—2021中7.4.2的相关内容。

9.1.13 支持终端节能

测试步骤和判定准则应符合GB/T 32420—2015中7.2.3.5的相关规定，并参照团体标准T/WAPIA 037.2—2021中7.3.5的相关内容。

9.1.14 自动信道选择

测试步骤和判定准则应符合GB/T 32420—2015中7.2.4.5的相关规定，并参照团体标准T/WAPIA 037.2—2021中7.4.5的相关内容。

9.1.15 分段门限设置

测试步骤和判定准则应符合GB/T 32420—2015中7.2.3.2的相关规定，并参照团体标准T/WAPIA 037.2—2021中7.3.2的相关内容。

9.1.16 用户权限

用户权限测试步骤和判定准则如下。

a) 测试步骤：

- 1) 以管理员身份登录一台出厂状态的AP, 输入默认管理员密码, 查看系统是否强制要求更改密码;
 - 2) 登录成功后退出, 尝试以错误的密码重新登录; 当连续输入三次错误的密码后, 查看登录功能是否被锁定;
 - 3) 修改管理员密码, 查看是否应输入原密码后才允许修改。
- b) 判定准则:
- 1) 测试步骤1) 中, 系统在首次登录时应强制要求修改管理员密码;
 - 2) 测试步骤2) 中, 系统应禁止登录; 且管理员密码连续输入错误三次后, 管理员账号登录功能应被锁定直至锁定时间结束;
 - 3) 测试步骤3) 中, 应输入原密码后, 才可以修改管理员密码。

9.1.17 身份鉴别

身份鉴别测试步骤和判定准则如下。

- a) 测试步骤:
- 1) 查看系统是否对所有登录用户进行身份标识和鉴别, 且至少使用用户名和静态口令的强度进行身份鉴别, 查看用户列表中的用户标识是否唯一;
 - 2) 查看系统管理员是否能够设置账号锁定及解锁策略(如三次登录失败至少20分钟后自动解锁或由授权的管理员进行解锁);
 - 3) 以某用户身份登录AP, 确保在管理员定义的一段时间内无会话活动后, 再次进行会话活动;
 - 4) 通过远程方式管理AP, 同时抓包查看管理端与AP间的所有通信数据是否加密。
- b) 判定准则:
- 1) 测试步骤1) 中, 系统对所有登录用户均使用用户名和静态口令, 或以上强度的方式进行了身份鉴别, 用户列表中用户标识唯一;
 - 2) 测试步骤2) 中, 可以查看到账号锁定及解锁策略管理功能, 用户在超过设定的登录失败次数后账号锁定;
 - 3) 测试步骤3) 中, 再次进行会话活动时, 应重新进行身份鉴别;
 - 4) 测试步骤4) 中, 抓包数据显示管理端与AP间的所有通信数据均被加密。

9.1.18 DoS 攻击

测试步骤和判定准则应符合GB/T 32420—2015中6.2.4.3.2的相关规定。

9.1.19 切断非法终端网络连接

测试步骤和判定准则应符合GB/T 32420—2015中6.2.4.2.2的相关规定。

9.2 接入点控制器

9.2.1 路由功能

路由功能测试步骤和判定准则如下。

- a) 测试步骤:
- 1) AC设置静态IPv4公网地址, 测试步骤应符合GB/T 21671—2018中6.1.3的相关规定;
 - 2) AC设置静态IPv6公网地址, 测试步骤应符合GB/T 21671—2018中6.1.3的相关规定。

b) 判定准则:

测试步骤1) 和7) 中的判定准则应符合GB/T 21671—2018中6.1.3的相关规定。

部署在公/私有云服务器的AC免测此项。

9.2.2 DHCP 功能

测试步骤和判定准则应符合GB/T 21671—2018中6.1.8的相关规定。

9.2.3 VLAN 功能

测试步骤和判定准则应符合GB/T 21671—2018中6.1.2的相关规定。

9.2.4 二层功能

9.2.4.1 STP 功能

测试步骤和判定准则应符合YD/T 1141—2007中7.1的相关规定。

部署在公/私有云服务器的AC免测此项。

9.2.4.2 链路聚合功能

测试步骤和判定准则应符合YD/T 1141—2007中5.4.3项目编号为99的相关规定。

部署在公有云服务器的AC免测此项。

9.2.5 三层功能

测试步骤和判定准则同9.1.3。

通过了三层交换机电信设备进网许可证并且进行了IPv6项目测试的AC设备，免测本项。

部署在公/私有云服务器的AC免测此项。

9.2.6 IPv4 协议

测试步骤和判定准则应符合YD/T 1098—2009中第11章的相关规定。

通过了三层交换机电信设备进网许可证的AC设备，免测本项。

部署在公/私有云服务器的AC免测此项。

9.2.7 IPv6 协议

测试步骤和判定准则应符合YD/T 1453—2014中第6章的相关规定。

通过了三层交换机电信设备进网许可证并且进行了IPv6项目测试的AC设备，免测本项。

部署在公/私有云服务器的AC免测此项。

9.2.8 设备发现方式

测试步骤和判定准则同9.1.2。

9.2.9 业务转发方式

测试步骤和判定准则同9.1.3。

9.2.10 速率控制

速率控制测试步骤和判定准则如下。

a) 测试步骤：

- 1) 登录AC管理界面，设置用户最大下载速度限值，该值应不超过网络出口带宽的50%；
- 2) 使用测速软件进行测速。

b) 判定准则：

测试步骤2)中，测速软件实测下载速度不应超过测试步骤1)中设置的最大下载速度限值。

9.2.11 强制下线

测试步骤和判定准则同9.1.9。

9.2.12 QoS 支持

测试步骤和判定准则同9.1.10。

9.2.13 管理 AP 功能

管理AP功能测试步骤和判定准则如下。

a) 测试步骤:

- 1) 登录AC管理界面, 查看是否支持对AP进行恢复出厂设置、重启和软件升级的操作;
- 2) 分别执行测试步骤1)中描述的操作, 验证是否生效。

b) 判定准则:

- 1) 测试步骤1)中, AC应支持测试步骤1)中描述的操作;
- 2) 测试步骤2)中, 测试步骤1)描述的操作应成功执行并验证生效。

9.2.14 AP 和 AC 间时间同步

AP和AC间时间同步测试步骤和判定准则如下。

a) 测试步骤:

- 1) 登录AC管理界面, 查看是否支持以NTP服务器的方式进行时间同步;
- 2) 执行与NTP服务器进行时间同步, 1 min后分别查看AP、AC的系统时间是否一致。

b) 判定准则:

- 1) 测试步骤1)中, AC应支持以NTP服务器的方式进行时间同步;
- 2) 测试步骤2)中, AP、AC的系统时间应与NTP服务器时间一致。

9.2.15 ACL

ACL测试步骤和判定准则如下。

a) 测试步骤:

- 1) 登录AC管理界面, 查看有无基于源IP、目的IP、源端口、目的端口的ACL策略设置项;
- 2) 任意设定ACL策略并下发AP执行, 查看AP是否按照ACL策略执行。

b) 判定准则:

- 1) 测试步骤1)中, AC应支持基于源IP、目的IP、源端口、目的端口的ACL策略设置项;
- 2) 测试步骤2)中, ACL策略应在AP侧执行生效。

9.2.16 用户权限

用户权限测试步骤和判定准则如下。

a) 测试步骤:

- 1) 使用默认账号、默认密码以管理员身份首次登录接入点控制器, 查看在首次登录成功后, 控制器是否立刻强制要求更改密码后重新登录;
- 2) 新创建一个拥有管理员权限的账号, 查看该账号是否可成功创建;
- 3) 停用测试步骤2)新创建的管理员账号, 查看是否可成功停用。

b) 判定准则:

- 1) 测试步骤1)中, 应以默认密码成功登录接入点控制器, 并立刻被强制更改默认密码, 以新密码成功登录;

- 2) 测试步骤2)中,新的管理员账号应被创建;
- 3) 测试步骤3)中,该管理员账号应被停用。

9.2.17 身份鉴别

身份鉴别测试连接图见图5。

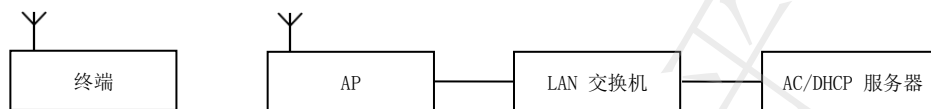


图5 身份鉴别测试连接图

测试步骤和判定准则如下。

a) 测试步骤:

- 1) 查看系统是否对所有登录用户进行身份标识和鉴别,且至少使用用户名和静态口令的强度进行身份鉴别,查看用户列表中的用户标识是否唯一;
- 2) 查看系统管理员是否能够设置账号锁定及解锁策略(如三次登录失败至少20分钟后自动解锁或由授权的管理员进行解锁);
- 3) 以某用户身份登录AC,并确保在管理员定义的一段时间内无会话活动后,再次进行会话活动;
- 4) 当通过远程方式进行管理AC时,抓包查看管理端与AC间的所有通信数据是否加密。

b) 判定准则:

- 1) 测试步骤1)中,系统对所有登录用户均使用用户名和静态口令,或以上强度的方式进行了身份鉴别,用户列表中用户标识唯一;
- 2) 测试步骤2)中,应查看到账号锁定及解锁策略管理功能,用户在超过设定的登录失败次数后账号被锁定;
- 3) 测试步骤3)中,再次进行会话活动时,应重新进行身份鉴别;
- 4) 测试步骤4)中,抓包数据显示管理端与AC间的所有通信数据均被加密。

9.2.18 网络访问安全

网络访问安全测试连接图见图5,测试步骤和判定准则如下。

a) 测试步骤:

- 1) 使终端成功接入无线网络,然后登录AC管理界面,将该终端MAC地址设置为黑名单,持续查看该终端的接入状态;
- 2) 登录AC管理界面,在白名单中指定允许接入的MAC地址;使用含有该MAC地址的终端和含有其它MAC地址的终端接入无线网络。

b) 判定准则:

- 1) 测试步骤1)中,黑名单生效,该终端最终不应接入无线网络;
- 2) 测试步骤2)中,白名单生效,含有允许接入的MAC地址的终端应接入无线网络,其它终端不应接入网络。

9.2.19 二层隔离功能

测试步骤和判定准则同9.1.7。

9.2.20 用户地址核查

用户地址核查测试连接图见图5，测试步骤和判定准则如下。

- a) 测试步骤：
 - 1) 使用AC分配DHCP地址池的方式组建无线网络，使终端成功接入网络并浏览网页；
 - 2) 使终端以静态IP地址方式重新接入无线网络，且该IP地址不在测试步骤1)中的DHCP地址池内。
- b) 判定准则：
 - 测试步骤2)中，终端不应接入无线网络。

9.2.21 非法用户检测

非法用户检测测试步骤和判定准则如下。

- a) 测试步骤：
 - 1) 使用非法用户登录，查看AC系统的帐户记录，确认是否记录该非法用户、IP访问信息；
 - 2) 配置黑名单为IP/MAC接入方式，使用含黑名单内IP/MAC的非法用户访问系统，查看是否有非法登录记录；
 - 3) 查看是否有未被授权的端口被开放或被监听；
 - 4) 使用非法用户登录，查看告警日志是否有非法用户访问记录。
- b) 判定准则：
 - 1) 测试步骤1)中，AC系统的账户记录中应存在该非法用户的登录记录和IP访问信息；
 - 2) 测试步骤2)中，黑名单生效，该非法用户不应访问访问系统，且存在该非法用户的登录记录；
 - 3) 测试步骤3)中，除授权端口外，系统应无其它端口被开放或被监听；
 - 4) 测试步骤4)中，告警日志中应存在非法用户访问记录。

9.2.22 安全审计

安全审计测试步骤和判定准则如下。

- a) 测试步骤：
 - 1) 设置AP允许终端访问信息上报，终端接入AP进行网页浏览；
 - 2) 登录AC管理界面，查看终端访问信息是否包含终端的IP地址、终端的MAC地址、AP的MAC地址、目的IP地址、目的端口、URL地址、协议、日期时间；
 - 3) 查看审计记录是否包括访问发生的日期和时间、主体、事件类型、事件结果；
 - 4) 查看是否支持存储访问日志，或将访问日志发往指定的日志服务器；
 - 5) 可选：查看是否支持将审计日志上送到公安网监平台。
- b) 判定准则：
 - 1) 测试步骤2)中，应查看到终端访问信息，访问信息包含终端的IP地址、终端的MAC地址、AP的MAC地址、目的IP地址、目的端口、协议、时间；
 - 2) 测试步骤3)中，审计记录应包括访问发生的日期和时间、主体、事件类型、事件结果如成功、失败；
 - 3) 测试步骤4)中，应支持存储终端访问日志，或将访问日志发往指定日志服务器；
 - 4) 测试步骤5)，应支持将审计日志上送到公安网监平台。

9.3 鉴别服务器

9.3.1 端口号

测试步骤和判定准则应符合GB/T 32420—2015中7.3.2的相关规定，并参照团体标准T/WAPIA 037.2—2021中8.2的相关内容。

9.3.2 证书管理

测试步骤和判定准则应符合GB/T 32420—2015中7.3.3.1的相关规定，并参照团体标准T/WAPIA 037.2—2021中8.3.1的相关内容。

9.3.3 MAC 地址绑定

测试步骤和判定准则应符合GB/T 32420—2015中7.3.3.4的相关规定，并参照团体标准T/WAPIA 037.2—2021中8.3.4的相关内容。

9.3.4 CRL 验证功能

CRL验证功能测试连接图见图6。

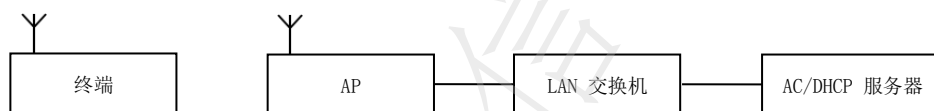


图6 CRL 验证测试连接图

测试步骤和判定准则如下。

- a) 测试步骤：
使用证书已吊销的终端连接WAPI网络。
- b) 判定准则：
终端不应接入WAPI网络。

9.3.5 漫游功能

测试步骤和判定准则应符合GB/T 32420—2015中7.3.3.7的相关规定，并参照团体标准T/WAPIA 037.2—2021中8.3.5的相关内容。

9.3.6 用户权限

测试步骤和判定准则应符合GB/T 28448—2019中7.1.4.2的相关规定。

9.3.7 安全审计

测试步骤和判定准则应符合GB/T 28448—2019中7.1.3.5的相关规定。

9.4 证书签发服务器

9.4.1 证书签发

测试步骤和判定准则应符合GB/T 32420—2015中7.3.3.1的相关规定，并参照团体标准T/WAPIA 037.2—2021中8.3.1的相关内容。

9.4.2 CRL 签发

CRL签发测试步骤和判定准则如下。

- a) 测试步骤：
 - 1) 在证书签发服务器的CRL管理界面，依据CRL签发策略签发CRL文件；

2) 在证书签发服务器的CRL管理界面, 执行CRL文件的查询和下载。

b) 判定准则:

1) 测试步骤1) 中, 应依据CRL签发策略成功签发CRL文件;

2) 测试步骤2) 中, 应查询到签发的CRL文件, 并成功下载该文件。

9.4.3 证书更新

测试步骤和判定准则应符合GB/T 32420—2015中7.1.3.8.6和7.2.3.8.5的相关规定。

9.4.4 证书查询

测试步骤和判定准则应符合GB/T 32420—2015中7.3.3.3的相关规定, 并参照团体标准T/WAPIA 037.2—2021中8.3.3的相关内容。

9.4.5 证书吊销

测试步骤和判定准则应符合GB/T 32420—2015中7.3.3.1的相关规定, 并参照团体标准T/WAPIA 037.2—2021中8.3.1的相关内容。

9.4.6 证书状态查询

测试步骤和判定准则应符合GB/T 32420—2015中7.3.3.3的相关规定, 并参照团体标准T/WAPIA 037.2—2021中8.3.3的相关内容。

9.4.7 用户权限

测试步骤和判定准则应符合GB/T 28448—2019中7.1.4.2的相关规定。

9.4.8 身份鉴别

测试步骤和判定准则应符合GB/T 28448—2019中7.1.4.1的相关规定。

9.4.9 安全审计

测试步骤和判定准则应符合GB/T 28448—2019中7.1.3.5的相关规定。

9.5 终端

9.5.1 扫描 AP

测试步骤和判定准则应符合GB/T 32420—2015中7.1.4.1的相关规定, 并参照团体标准T/WAPIA 037.2—2021中6.4.1的相关内容。

9.5.2 分段门限设置

测试步骤和判定准则应符合GB/T 32420—2015中7.1.3.2的相关规定, 并参照团体标准T/WAPIA 037.2—2021中6.3.2的相关内容。

9.5.3 RTS 门限设置

测试步骤和判定准则应符合GB/T 32420—2015中7.1.3.3的相关规定, 并参照团体标准T/WAPIA 037.2—2021中6.3.3的相关内容。

9.5.4 节能功能

测试步骤和判定准则应符合GB/T 32420—2015中7.1.3.4的相关规定，并参照团体标准T/WAPIA 037.2—2021中6.3.4的相关内容。

9.5.5 同一 AS 域内 AP 间切换功能

测试步骤和判定准则应符合GB/T 32420—2015中7.1.4.3的相关规定，并参照团体标准T/WAPIA 037.2—2021中6.4.3相关内容。

9.5.6 QoS 功能

测试步骤和判定准则应符合GB/T 32420—2015中7.1.3.5的相关规定，并参照团体标准T/WAPIA 037.2—2021中6.3.5的相关内容。

9.5.7 组播功能

测试步骤和判定准则应符合GB/T 32420—2015中7.1.3.6的相关规定，并参照团体标准T/WAPIA 037.2—2021中6.3.6的相关内容。

10 性能测试

10.1 无线接入点

10.1.1 吞吐量

测试步骤和判定准则应符合GB/T 32420—2015中7.2.5.1的相关规定，并参照团体标准T/WAPIA 037.2—2021中7.5.1的相关内容。

10.1.2 用户容量

用户容量测试连接图见图7。



图7 用户容量测试连接图

预置条件、测试步骤和判定准则如下。

a) 预置条件：

- 1) 准备64台终端，可以采用真实物理终端或虚拟仿真终端仪表设备；
- 2) 准备流量发生器，能够发送TCP/UDP流量报文；
- 3) 准备一台微型计算机可以通过有线网络与AP处于所在IP网络。

b) 测试步骤：

- 1) 设置无线接入点的射频模式为IEEE 802.11n；
- 2) 设置64台终端接入AP，观察并记录能够同时接入AP的终端总数；
- 3) 使用流量发生器进行PC到终端的TCP下行流量测试；逐步增加流量测试的终端个数，观察并记录可同时有流量的终端个数和终端流量大小；
- 4) 使用流量发生器进行终端到PC的TCP上行流量测试；逐步增加流量测试的终端个数，观察并记录可同时有流量的终端个数和终端流量大小；
- 5) 如AP支持IEEE 802.11ac，设置AP的射频模式为IEEE 802.11ac，重复测试步骤2)～4)；

- 6) 如AP支持IEEE 802.11ax, 设置AP的射频模式为IEEE 802.11ax, 重复测试步骤2)~4)。
- c) 判断准则:
测试步骤2)~6)应符合T/WAPIA 040.1—2020中6.6.1要求的相关内容。

10.2 接入点控制器

10.2.1 吞吐量

测试步骤应符合GB/T 21671—2018中6.2.3.1的相关规定, 判定准则应符合T/WAPIA 040.1—2020中7.6.1的相关内容。

10.2.2 接入控制能力

10.2.2.1 转发时延

测试步骤应符合GB/T 21671—2018中6.2.5的相关规定, 判定准则应符合T/WAPIA 040.1—2020中7.6.2 d)的相关内容。

10.2.2.2 DHCP 性能

测试步骤应符合GB/T 21671—2018中6.3.1.1的相关规定, 判定准则应符合T/WAPIA 040.1—2020中7.6.3的相关内容。

10.2.3 热备或集群部署

热备或集群部署测试步骤和判定准则如下。

a) 测试步骤:

- 1) 部署双机备份AC, 主、备两台AC均为运行状态;
- 2) 访问主AC, 并持续执行业务操作;
- 3) 关闭主AC。

b) 判定准则:

测试步骤3)中, 在持续执行业务操作期间, 应对主、备AC切换过程无明显感知, 并记录切换时间(精确到毫秒)。

10.3 鉴别服务器

10.3.1 鉴别性能

鉴别性能测试步骤和判定准则如下。

a) 测试步骤:

使用性能测试工具, 对数字证书认证接口进行有效鉴别并发数测试。

b) 判定准则:

性能测试工具应正确完成有效鉴别并发数测试, 并记录测试结果(次/秒)。

10.3.2 热备

10.3.2.1 1:1 备份倒换时间

1:1备份倒换时间测试步骤和判定准则如下。

a) 测试步骤:

- 1) 部署1:1备份鉴别服务器, 主、备两台鉴别服务器均为运行状态;
- 2) 用户访问主鉴别服务器, 并持续执行业务操作;

3) 关闭主服务器。

b) 判定准则：

测试步骤3)中，在持续执行业务操作期间，用户应对关闭主服务器的过程无明显感知，并记录倒换时间，（精确到毫秒）。

10.4 证书签发服务器

10.4.1 证书容量

证书容量测试步骤和判定准则如下。

a) 测试步骤：

- 1) 证书签发服务器应提供自动化测试脚本程序，该脚本部署于独立的服务器中。该服务器应与证书签发服务器网络连通；
- 2) 在自动化测试脚本程序中配置证书测试数量，启动脚本进行证书签发量测试。

b) 判定准则：

测试步骤2)中，自动化测试脚本程序应正确完成测试，并记录证书签发数量。

10.5 终端

10.5.1 吞吐量

测试步骤和判定准则应符合GB/T 32420—2015中7.1.5.1的相关规定，并参照团体标准T/WAPIA 037.2—2021中6.5.1的相关内容。

10.5.2 时延

测试步骤和判定准则应符合GB/T 32420—2015中7.1.5.2的相关规定，并参照团体标准T/WAPIA 037.2—2021中6.5.2的相关内容。

10.5.3 抖动

测试步骤和判定准则应符合GB/T 32420—2015中7.1.5.3的相关规定，并参照团体标准T/WAPIA 037.2—2021中6.5.3的相关内容。

10.5.4 丢包率

测试步骤和判定准则应符合GB/T 32420—2015中7.1.5.4的相关规定，并参照团体标准T/WAPIA 037.2—2021中6.5.4的相关内容。

附 录 A
(资料性)
技术要求与测试方法对照表

A.1 无线接入点测试

T/WAPIA 040.1—2020中规定的无线接入点技术要求与本文件规定的无线接入点测试方法其章条对应关系见表A.1。

表A.1 无线接入点测试项目对照表 (第1页/共3页)

序号	T/WAPIA 040.1—2020 技术要求索引	技术要求名称	测试方法索引	备注
1	6.1	基本要求	-	
2	6.2.1	网络侧物理接口	7.1	
3	6.2.2	用户侧物理接口	7.2	
4	6.3.1	IP协议支持能力	9.1.1	
5	6.3.2	IPv4功能	9.1.1	
6	6.3.3	IPv6功能	9.1.1	
7	6.3.4	AC发现方式	9.1.2	
8	6.3.5	业务转发方式	9.1.3	
9	6.3.6	漫游切换支持能力	9.1.4	
10	6.3.7	功率控制	9.1.5	
11	6.3.8 a)	简单接入控制能力	9.1.6.2	
12	6.3.8 b)	限制最大关联用户数	9.1.6.3	
13	6.3.8 c)	多SSID能力	9.1.6.4	
14	6.3.9	用户隔离功能	9.1.7	
15	6.3.10	VLAN支持能力	9.1.8	
16	6.3.11	QoS支持能力	9.1.10	
17	6.3.12 a)	WLAN功能启用和禁用	-	
18	6.3.12 b)	SSID中文/英文编码	6.1	
19	6.3.12 c)	信标间隔设置	9.1.11	
20	6.3.12 d)	动态速率切换	9.1.12	
21	6.3.12 e)	支持终端节能	9.1.13	
22	6.3.12 f)	自动信道选择	9.1.14	
23	6.3.12 g)	发射功率可调	-	
24	6.3.12 h)	无线终端访问隔离	-	
25	6.3.12 i)	无线工作模式	-	
26	6.3.12 j)	分段门限设置	9.1.15	
27	6.3.12 k)	天线可选内置/外置	-	
28	6.4.1 a)	ACL功能	-	

表A.1 无线接入点测试项目对照表（第2页/共3页）

序号	T/WAPIA 040.1—2020 技术要求索引	技术要求名称	测试方法索引	备注
29	6.4.1 b)	报文过滤功能	-	
30	6.4.1 c)	防DoS攻击	9.1.18	
31	6.4.1 d)	防端口扫描功能	-	
32	6.4.1 e)	防非法报文攻击功能	-	
33	6.4.2 a)	SSID配置	6.1	
34	6.4.2 b)	WAPI证书安装	6.2	
35	6.4.2 b)	WAPI-PSK接入	6.3	
36	6.4.2 b)	WAPI-Cert接入	6.4	
37	6.4.2 b)	加密传输	6.5	
38	6.4.2 b)	密钥更新	6.6	
39	6.4.2 b)	密钥存储	-	
40	6.4.2 c)	错误帧帧处理	-	
41	6.4.2 c)	错误空数据帧处理	-	
42	6.4.2 d)	强制STA下线	9.1.9	
43	6.4.2 e)	否定非法证书	6.7	
44	6.4.2 f)	MAC地址过滤	-	
45	6.4.2 g)	切断非法终端网络连接	9.1.19	
46	6.5.1	基本要求	-	
47	6.5.2	日志要求	-	
48	6.5.3	配置文件备份	-	
49	6.5.4 a)	设备状态	-	
50	6.5.4 b)	设备日志	-	
51	6.5.5 a)	管理员管理	9.1.16	
52	6.5.5 b)	日志文件管理	-	
53	6.5.5 c)	软件、固件升级	-	
54	6.5.5 d)	设备重启功能	-	
55	6.5.5 e)	恢复出厂设置功能	-	
56	6.5.6	网络诊断	-	
57	6.5.7	身份鉴别	9.1.17	
58	6.6.1	用户容量	10.1.2	
59	6.6.2	吞吐量	10.1.1	
60	6.6.3	时延	-	
61	6.6.4	抖动	-	
62	6.6.5	丢包率	-	
63	6.6.6	接收灵敏度	-	
64	6.6.7	可靠性	-	
65	6.6.8	其他要求	-	
66	6.7.1	工作温度	8.1.1	
67	6.7.2	存储温度	8.1.2	

表A.1 无线接入点测试项目对照表（第3页/共3页）

序号	T/WAPIA 040.1—2020 技术要求索引	技术要求名称	测试方法索引	备注
68	6.7.3	工作湿度	8.1.3	
69	6.7.4	存储湿度		
70	6.7.5	防尘防水等级	-	
71	6.7.6	大气压	-	
72	6.7.7	抗风强度	-	
73	6.7.8	机械环境适应性	-	
74	6.7.9	接地	-	
75	6.7.10	电磁兼容性	8.2	
76	6.7.11	绝缘电阻	-	
77	6.7.12	运行电气条件	-	

A.2 接入点控制器测试

T/WAPIA 040.1—2020中规定的接入点控制器技术指标与本文件规定的接入点控制器测试方法其条款对应关系见表A.2。

表A.2 接入点控制器测试项目对照表（第1页/共2页）

序号	T/WAPIA 040.1—2020 技术要求索引	技术要求名称	测试方法索引	备注
1	7.1	基本要求	-	
2	7.2	物理接口要求	7.1	
3	7.3.1	路由功能	9.2.1	
4	7.3.2	WAPI功能	6	参照接入点测试方法进行测试
5	7.3.3	DHCP功能	9.2.2	
6	7.3.4	VLAN功能	9.2.3	
7	7.3.5	二层功能	9.2.4	
8	7.3.6	三层功能	9.2.5	
9	7.3.7	IPv4支持能力	9.2.6	
10	7.3.8	IPv6支持能力	9.2.7	
11	7.3.9	设备发现功能	9.2.8	
12	7.3.10	业务转发	9.2.9	
13	7.3.11	速率控制	9.2.10	
14	7.3.12	强制下线	9.2.11	
15	7.3.13	QoS功能	9.2.12	
16	7.3.14	管理AP功能	9.2.13	
17	7.3.15	同步要求	9.2.14	
18	7.3.16	扩展要求	-	
19	7.4.1	接入控制	9.2.15	

表A.2 接入点控制器测试项目对照表（第1页/共2页）

序号	T/WAPIA 040.1—2020 技术要求索引	技术要求名称	测试方法索引	备注
20	7.4.2	网络访问安全	9.2.18	
21	7.4.3	二层隔离要求	9.2.19	
22	7.4.4	WLAN防非法攻击能力	-	
23	7.4.5	非法AP检测	-	
24	7.4.6	防止假冒能力	-	
25	7.4.7	防DoS攻击	-	
26	7.4.8	用户地址核查	9.2.20	
27	7.5.1	操作维护功能	-	
28	7.5.2	网管功能	-	
29	7.5.3	日志要求	-	
30	7.5.4	远程故障诊断	-	
31	7.5.5 a)	管理员管理	-	
32	7.5.5 b)	设备重启功能	-	
33	7.5.5 c)	恢复出厂设置功能	-	
34	7.5.5 d)	信息可视化	-	
35	7.5.6	身份鉴别	9.2.17	
36	7.5.7	安全审计	9.2.22	
37	7.6.1	吞吐量	10.2.1	
38	7.6.2	无线控制	-	
39	7.6.3	接入控制	10.2.2	
40	7.6.4	稳定性	-	
41	7.6.5	可靠性	-	
42	7.6.6	可用性	-	
43	7.7.1	工作温度	8.1.1	
44	7.7.2	存储温度	8.1.2	
45	7.7.3	工作湿度	8.1.3	
46	7.7.4	存储湿度	-	
47	7.7.5	大气压	-	
48	7.7.6	电磁兼容性	8.2	
49	7.7.7	运行电气条件	-	

A.3 鉴别服务器测试

T/WAPIA 040.1—2020中规定的鉴别服务器技术指标与本文件规定的鉴别服务器测试方法其章条对应关系见表A.3。

表A.3 鉴别服务器测试项目对照表

序号	T/WAPIA 040.1—2020 技术要求索引	技术要求名称	测试方法索引	备注
1	8.1	基本要求	—	
2	8.2	物理接口要求	7.1	
3	8.3.1	协议流程和数据格式	6.4	
4	8.3.2	设备信息管理	—	
5	8.3.3	证书管理	9.3.2	
6	8.3.4	授权管理	—	
7	8.3.5	证书鉴别	6.4 9.3.3	
8	8.3.6	CIS证书同步	—	
9	8.3.7	与CIS安全通信功能	—	
10	8.3.8	CRL验证	9.3.4	
11	8.3.9	漫游功能	9.3.5	
12	8.3.10	端口号	9.3.1	
13	8.3.11	数据备份和恢复	—	
14	8.4.1	系统要求	—	
15	8.4.2	密码算法	—	
16	8.4.3	证书及密钥管理	—	
17	8.4.4	安全管理	—	
18	8.4.5	物理安全防护	—	
19	8.5.1	管理员管理	—	
20	8.5.2	日志要求	—	
21	8.5.3	安全审计	9.3.7	
22	8.6.1	鉴别性能	10.3.1	
23	8.6.2	可靠性	—	
24	8.6.3	可用性	—	
25	8.7.1	工作温度	8.1.1 8.1.2 8.1.3	
26	8.7.2	存储温度		
27	8.7.3	工作湿度		
28	8.7.4	存储湿度		
29	8.7.5	大气压	—	
30	8.7.6	电磁兼容性	8.2	
31	8.7.7	运行电气条件	—	

A.4 证书签发服务器测试

T/WAPIA 040.1—2020中规定的证书签发服务器技术指标与本文件规定的证书签发服务器测试方法其章条对应关系见表A.4。

表A.4 证书签发服务器测试项目对照表

序号	T/WAPIA 040.1—2020 技术要求索引	技术要求名称	测试方法索引	备注
1	9.1	基本要求	-	
2	9.2	物理接口要求	7.1	
3	9.3.1	证书签发	9.4.1	
4	9.3.2	CRL签发	9.4.2	
5	9.3.3	证书更新	9.4.3	
6	9.3.4	证书查询功能	9.4.4	
7	9.3.5	证书吊销功能	9.4.5	
8	9.3.6	证书状态查询	9.4.6	
9	9.3.7	设备信息管理	-	
10	9.3.8	授权管理	-	
11	9.3.9	统计分析功能	-	
12	9.3.10	数据备份和恢复	-	
13	9.3.11	与AS安全通信功能	-	
14	9.4.1	系统要求	-	
15	9.4.2	密码算法	-	
16	9.4.3	安全管理	-	
17	9.4.4	物理安全防护	-	
18	9.5.1	管理员管理	-	
19	9.5.2	日志要求	-	
20	9.5.3	安全审计	9.4.9	
21	9.6.1	证书容量	10.4.1	
22	9.6.2	可靠性	-	
23	9.6.3	可用性	-	
24	9.7.1	工作温度	8.1.1	
25	9.7.2	存储温度	8.1.2	
26	9.7.3	工作湿度	8.1.3	
27	9.7.4	存储湿度		
28	9.7.5	大气压	-	
29	9.7.6	电磁兼容性	8.2	
30	9.7.7	运行电气条件	-	

A.5 终端测试

T/WAPIA 040.1—2020中规定的终端技术指标与本文件规定的终端器测试方法其章条对应关系见表A.5。

表A.5 终端测试项目对照表

序号	T/WAPIA 040.1—2020 技术要求索引	技术要求名称	测试方法索引	备注
1	10.1	基本要求	-	
2	10.2	物理接口要求	7.2	
3	10.3.1	扫描AP功能	9.5.1	
4	10.3.2	SSID配置	6.1	
5	10.3.3	分段门限设置	9.5.2	
6	10.3.4	RTS门限设置	9.5.3	
7	10.3.5	节能功能	9.5.4	
8	10.3.6 a)	证书安装	6.2	
9	10.3.6 b)	证书选择功能	6.8	
10	10.3.6 c)	证书鉴别功能	6.4	
11	10.3.6 d)	加密功能	6.5	
12	10.3.6 e)	密钥更新功能	6.6	
13	10.3.6 f)	否定非法证书功能	6.7	
14	10.3.7	同一AS域内AP间切换功能	9.5.5	
15	10.3.8	QoS功能	9.5.6	
16	10.3.9	组播功能	9.5.7	
17	10.4 a)	WAPI-PSK接入	6.3	
18	10.4 b)	WAPI-Cert接入	6.4	
19	10.4 c)	加密传输	6.5	
20	10.4 d)	密钥更新	6.6	
21	10.4 e)	密钥存储	-	
22	10.5.1	吞吐量	10.5.1	
23	10.5.2	时延	10.5.2	
24	10.5.3	抖动	10.5.3	
25	10.5.4	丢包率	10.5.4	
26	10.5.5	接收灵敏度	-	
27	10.6.1	工作温度	8.1.1 8.1.2 8.1.3	
28	10.6.2	存储温度		
29	10.6.3	工作湿度		
30	10.6.4	存储湿度		
31	10.6.5	大气压	-	
32	10.6.6	电磁兼容性	8.2	
33	10.6.7	运行电气条件	-	