

团体标准

T/WAPIA 040.1—2020

关键信息基础设施无线局域网技术要求 第1部分：通用要求

WLAN technical requirements of critical information infrastructure
Part 1: General requirements

2020-12-15 发布

2020-12-15 实施

中关村无线网络安全产业联盟 发布

目 次

版权声明	III
前言	IV
引言	V
1 范围	1
2 规范性引用文件	1
3 术语与定义	2
4 符号与缩略语	2
5 网络技术要求	3
5.1 组网技术	4
5.2 组网要求	4
5.3 网络安全	4
5.4 网络传输性能	4
5.5 IP 地址	4
5.6 VLAN 规划	4
5.7 频率规划	5
5.8 等级保护	5
6 无线接入点	5
6.1 基本要求	5
6.2 物理接口要求	5
6.3 功能要求	6
6.4 安全要求	7
6.5 管理和维护要求	8
6.6 性能要求	9
6.7 运行环境要求	12
7 接入点控制器	13
7.1 基本要求	13
7.2 物理接口要求	13
7.3 功能要求	14
7.4 安全要求	15
7.5 管理和维护要求	16
7.6 性能要求	17
7.7 运行环境要求	17
8 鉴别服务器	18
8.1 基本要求	18
8.2 物理接口要求	18
8.3 功能要求	18
8.4 安全要求	19
8.5 管理和维护要求	19
8.6 性能要求	19

8.7 运行环境要求	20
9 证书签发服务器	20
9.1 基本要求	20
9.2 物理接口要求	20
9.3 功能要求	20
9.4 安全要求	21
9.5 管理和维护要求	21
9.6 性能要求	21
9.7 运行环境要求	22
10 终端	22
10.1 基本要求	22
10.2 物理接口要求	22
10.3 功能要求	22
10.4 安全要求	23
10.5 性能要求	23
10.6 运行环境要求	24

WAPI Alliance
产 | 业 | 联 | 盟

版权声明

本文件版权归WAPI产业联盟（中关村无线网络安全产业联盟）©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
产 | 业 | 联 | 盟

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》的规定起草。

本文件是 T/WAPIA 040《关键信息基础设施无线局域网技术要求》的第1部分。

本文件由 WAPI 产业联盟（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，由无线网络安全标准化委员会归口。

本文件起草单位：WAPI 产业联盟（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、广州广电计量检测股份有限公司、北京数字认证股份有限公司、深圳市信锐网科技术有限公司、北京华信傲天技术股份有限公司、深圳市瑞科慧联科技有限公司、新华三技术有限公司、南方电网科学研究院有限责任公司、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、天津市无线电监测站、中国电信股份有限公司研究院、高通无线通信技术（中国）有限公司、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、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）、湖北经济学院。

本文件主要起草人：张国强、简练、张变玲、黄振海、张璐璐、方帅、严敏辉、肖笃亮、侯鹏亮、范小伟、谭鑫、禹凯、郑骊、刘婷、张海涛、匡晓云、尹玉昂、杨韬、高德龙、李楠、蓝海昌、袁成、高波、王江胜、许昱、赵天旭、任成龙、周园、王立华、周涛、索思亮、陈立明、黄开天、姜敏、陈晓龙、陈维刚、潘琪、葛珊、卢杰、祝张睿、孙宝林。

引 言

随着网络安全法、密码法和网络安全等级保护 2.0 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 技术和产品保障网络安全的需求，得到了越来越广泛的应用。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。WAPI 产业联盟无线网络安全标准化委员会组织开展了 T/WAPIA 040《关键信息基础设施无线局域网技术要求》系列团体标准的制定工作。

针对行业应用需求，联盟成员单位和业内厂商迫切需要一份明确的技术要求，规范无线局域网技术在关键基础设施中的应用，确保产品设计、生产和采购、部署等环节的合规性和一致性。

《关键信息基础设施无线局域网技术要求》旨在制定引用于关键信息基础设施的无线局域网系统及设备的技术要求，给联盟成员单位、业内厂商以及电力等行业部门、机构等提供准确、完整的指南，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 040 拟由如下几部分构成。

——第 1 部分：通用要求。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技术要求。

——第 2 部分：电力行业扩展要求。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技术要求。

将来可能会随着技术的变化添加新的部分阐述特定领域的特殊要求。

WAPI Alliance
产 | 业 | 联 | 盟

关键信息基础设施无线局域网技术要求 第1部分：通用要求

1 范围

本文件规定了在关键信息基础设施及相关环境中应用无线局域网的基本技术要求。

本文件适用于无线局域网设备的设计、生产和采购，也适用于行业无线局域网的建设和监督管理。

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 1988 信息技术 信息交换用七位编码字符集

GB/T 4208 外壳防护等级 (IP代码)

GB/T 9254 信息技术设备的无线电骚扰限值和测量方法

GB 15629.11—2003 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 15629.11—2003/XG1—2006 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 第1号修改单

GB 15629.1101—2006 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：5.8 GHz频段高速物理层扩展规范

GB 15629.1102—2003 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：2.4 GHz频段较高速物理层扩展规范

GB/T 15629.1103—2006 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：附加管理域操作规范

GB 15629.1104—2006 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：2.4 GHz频段更高数据速率扩展规范

GB 15629.3—2014 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3部分：带碰撞检测的载波侦听多址访问 (CSMA/CD) 的访问方法和物理层规范

GB/T 16264.8—2005 信息技术 开放系统互连 目录 第8部分：公钥和属性证书框架

GB/T 17618 信息技术设备 抗扰度 限值和测量方法

GB/T 17625.1 电磁兼容 限值 谐波电流发射限值（设备每相输入电流≤16A）

GB/T 17626.5 电磁兼容 试验和测量技术 浪涌（冲击）抗扰度试验

GB 18030 信息技术 中文编码字符集

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 32420—2015 无线局域网测试规范

GM/T 0014 数字证书认证系统密码协议规范

YD/T 1312.2—2004 无线通信设备电磁兼容性要求和测量方法 第2部分：宽带无线电设备

YD/T 1484 移动台空间射频辐射功率和接收机性能测量方法

YD/T 3168 公众无线局域网设备射频指标技术要求和测试方法

T/WAPIA 007.1—2010 无线局域网产品工程化实现指南 第1部分：WAPI与IEEE 802.11n

T/WAPIA 007.1—2010/XG1—2014 无线局域网产品工程化实现指南 第1部分：WAPI与IEEE 802.11n 第1号修改单

T/WAPIA 007.8—2016 无线局域网产品工程化实现指南 第8部分：WAPI与IEEE 802.11ac

T/WAPIA 007.10—2020 无线局域网产品工程化实现指南 第8部分：WAPI与IEEE 802.11ax

T/WAPIA 010.2—2010 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：2.4 GHz频段更高数据速率扩展规范 补篇2：无线局域网证书鉴别漫游规范

IEEE 802.3af 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3部分：带冲突检测(CSMA/CD)的载波侦听多路访问方法和物理层规范 数据终端设备(DTE)通过媒体相关接口(MDI)供电 (IEEE Standard for Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific Requirements – Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications – Data Terminal Equipment (DTE) Power Via Media Dependent Interface (MDI))

IEEE 802.3at 信息技术标准 局域网和城域网 特定要求 第3部分：带冲突检测(CSMA/CD)的载波侦听多路访问方法和物理层规范 修订3：数据终端设备(DTE)通过媒体相关接口(MDI)供电增强功能 (IEEE Standard for Information technology – Local and metropolitan area networks – Specific requirements – Part 3: CSMA/CD Access Method and Physical Layer Specifications Amendment 3: Data Terminal Equipment (DTE) Power via the Media Dependent Interface (MDI) Enhancements)

IEEE 802.3bt 以太网标准 修订2：4对以太网供电的物理层和管理参数 (IEEE Standard for Ethernet Amendment 2: Physical Layer and Management Parameters for Power over Ethernet over 4 pairs)

IEEE 802.1Q 局域网和城域网 桥和虚拟桥接网络 (IEEE Standard for Local and metropolitan area networks – Bridges and Bridged Networks)

RFC 2131 动态主机配置协议 (Dynamic Host Configuration Protocol)

PKCS #10 认证请求语法规则 (Certification Request Syntax Specification)

3 术语与定义

GB 15629.11系列国家标准界定的以及下列术语和定义适用于本文件。

3.1

接入点控制器 ap controller

提供对AP的集中控制管理、包括版本下发、配置下发、射频管理和用户流量管理。

3.2

鉴别服务器 authentication server

为终端和AP提供身份鉴别服务。

3.3

证书签发服务器 certificate issue server

提供对无线局域网STA、AP和AS的证书签发管理，包括证书签发、CRL签发、证书吊销、证书查询和证书更新等管理。

3.4

终端 terminal

包含符合GB 15629.11系列MAC和物理层规范的无线局域网STA功能模块的设备。

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)
ASU	鉴别服务单元 (authentication service unit)
CIS	证书签发服务器 (certificate issue server)
CISU	证书签发服务单元 (certificate issue service unit)
CPE	客户终端设备 (customer premise equipment)
CRC	循环冗余校验 (cyclic redundancy check)
CRL	证书吊销列表 (certificate revocation list)
CAPWAP	无线接入点的控制和配置协议 (control and provisioning of wireless access points protocol specification)
DHCP	动态主机配置协议 (dynamic host configuration protocol)
DNS	域名系统 (domain name system)
DoS	拒绝服务 (denial of service)
DSCP	差分业务编码 (differentiated services codepoint)
FTP	文件传输协议 (file transfer protocol)
ICMP	互联网控制报文协议 (internet control message protocol)
IP	互联网协议 (internet protocol)
LACP	链路汇聚控制协议 (link aggregation control protocol)
LAN	局域网 (local area network)
MAC	媒体访问控制 (medium access control)
MIB	管理信息库 (management information base)
Modbus	Modbus 协议 (modbus protocol)
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)
OSPF	开放式最短路径优先 (open shortest path first)
PEM	增强的保密邮件 (privacy enhanced mail)
PKCS	公钥密码标准 (the public-key cryptography standard)
PoE	以太网供电 (power over ethernet)
QoS	服务质量 (quality of service)
RIP	路由信息协议 (routing information protocol)
RTS	请求发送 (request to send)
SLAAC	无状态地址自动配置 (stateless address autoconfiguration)
SNMP	简单网络管理协议 (simple network management protocol)
SSID	服务集标识 (service set identifier)
STA	站 (点) (station)
UDP	用户数据报协议 (user datagram protocol)
VLAN	虚拟局域网 (virtual local area network)
WAI	无线局域网鉴别基础结构 (wlan authentication infrastructure)
WAPI	无线局域网鉴别与保密基础结构 (wlan authentication and privacy infrastructure)
WLAN	无线局域网 (wireless local area network)
WPI	无线局域网保密基础结构 (wlan privacy infrastructure)

5 网络技术要求

5.1 组网技术

WLAN无线接入系统主要由无线接入点（AP）、接入点控制器（AC）、鉴别服务器（AS）和证书签发服务器（CIS）组成。

AP是无线用户的接入点。

AC主要完成WLAN用户接入控制和无线控制等功能，其中无线控制可包括射频资源管理、AP设备管理、切换控制、安全功能和无线业务控制等功能。不同部署场景下，AC功能范围也不同，AC的部分功能需要和AP配套实现。

AP和AC协同实现终端的接入和管理，如对终端的身份鉴别、漫游管理、数据传输及日志生成与上报等。后续章节对可协同实现的功能技术要求在无线接入点章节中列出，该功能在AC中实现也应符合本规范中相关内容的规定。

AS主要完成STA和AP的身份鉴别。

AS的核心功能模块ASU主要完成对证书合法性的鉴别，具体在应用部署时根据网络规模可选择单台专用设备AS或将ASU集成到AP中。

CIS的核心功能模块CISU主要完成对无线局域网STA、AP和AS的证书签发管理。具体在应用部署时根据网络规模可选择单台专用设备或包含了CISU的通用设备，或由多台专用或通用设备构成的证书签发服务系统，CISU也可以被集成到AS中。

5.2 组网要求

本项要求包括：

- a) 稳定性：无线局域网的系统分组丢失率应低于 10^{-5} ，误码率应低于 10^{-8} ；
- b) 兼容性：对于室内使用的无线局域网，应使其跟现有的有线局域网在网络操作系统和网络软件上相互兼容；
- c) 数据速率：为了满足局域网业务量的需要，应保障无线局域网的数据传输速率；
- d) 通信保密：由于数据通过无线介质在空中传播，无线局域网应在不同层次采取有效的措施以提高通信保密和数据安全性能；
- e) 移动性：支持全移动网络或半移动网络；
- f) 节能管理：当无数据收发时使站点机处于休眠状态，当有数据收发时再激活，从而达到节省电力消耗的目的；
- g) 电磁环境：无线局域网部署应考虑电磁对周边环境的影响问题。

5.3 网络安全

为保障无线局域网的安全，应采用GB 15629.11系列国家标准规范的WAPI安全协议，并符合GB/T 32420—2015。应分别对局域网中无线接入点、接入点控制器、鉴别服务器、证书签发服务系统和终端做安全要求，详见各章节安全要求。

5.4 网络传输性能

为保障无线局域网业务运行，应分别对无线接入点、接入点控制器、鉴别服务器、证书签发服务系统和终端做性能要求，详见各章节性能要求。

5.5 IP 地址

本项要求包括：

- a) 终端的IP采用AC或独立DHCP server自动分配的地址；
- b) AC管理地址采用静态手工配置或DHCP server自动分配的地址，该地址用于AC和AP之间以CAPWAP等方式建立连接；
- c) AP的IP地址采用AC或独立DHCP server自动分配的地址。其中DHCP server可以由AC提供，也可以利用单独的DHCP server服务器，推荐使用AC进行统一分配；
- d) AP与AC之间如果经过三层转发，中间三层设备应支持DHCP RELAY。

5.6 VLAN 规划

本项要求包括：

- a) AP应根据AC下发的业务VLAN配置信息为业务流添加VLAN标签(tag)，可封装到通信隧道(CAPWAP等)中；
- b) AC应将通信隧道(CAPWAP等)中的业务流解包并转发，终结VLAN。

5.7 频率规划

本项要求包括：

- a) WLAN频率规划应符合国家标准GB 15629.11—2003、GB 15629.1101—2006、GB 15629.1102—2003、GB 15629.1104—2006和团体标准T/WAPIA 007.1—2010、T/WAPIA 007.1—2010/XG1—2014、T/WAPIA 007.8—2016、T/WAPIA 007.10—2020相关要求；

- b) WLAN频率分配要求包括：

- 1) 采用同一频点组中的不重叠频点进行频点规划；
- 2) 相邻覆盖区的AP不能使用相同频点；
- 3) 相同频点通过间隔较远距离或建筑物隔断增加同频隔离度，避免同频干扰；
- 4) 部分热点考虑整体容量，在满足载干比要求的情况下增加AP数量，采用频点紧凑复用的方式增加容量。

- c) WLAN频率规划可采用如下几种覆盖模式：

- 1) 室外覆盖方式

室外覆盖方式一般采用定向天线，针对覆盖区域定向覆盖，频率规划需要将相邻覆盖区域采用不同信道覆盖。以避免覆盖区产生同频干扰而造成网络质量下降。

- 2) 室内放装方式

中小型空间需要布放AP数量少，按照频点不重叠排列规划即可；大型空旷区域需要多个AP时，按照每个AP覆盖区域采用空间间隔的方法实现不重叠频点的频率重复利用。

对于大型有阻挡物的区域，要根据阻挡物情况充分利用阻挡物实现不重叠信道的重复利用。

- 3) 合路室内分布方式

合路室内分布方式，WLAN信号是从室内分布天线输出，需要根据天线布放情况选择合路点，对整体网络做信道规划。应从支路合路，每台AP所带天线相对集中。这样频率规划更容易。

5.8 等级保护

行业无线局域网系统应符合GB/T 22239标准相关要求。

6 无线接入点

6.1 基本要求

本项要求包括：

- a) AP与STA之间的空中接口物理层应符合国家标准GB 15629.11—2003、GB 15629.1102—2003、GB 15629.1104—2006、GB 15629.1101—2006和团体标准T/WAPIA 007.1—2010、T/WAPIA 007.1—2010/XG1—2014、T/WAPIA 007.8—2016、T/WAPIA 007.10—2020；
- b) 工作在2.4 GHz频段的AP工作频率范围为2400 MHz~2483.5 MHz；
- c) 工作在5 GHz频段的AP工作频率范围为5150 MHz~5350 MHz和5725 MHz~5850 MHz；
- d) 支持2.4 GHz/5 GHz双频的AP宜支持双频同时工作；
- e) AP应获得国家无线电主管部门颁发的型号核准证书。

6.2 物理接口要求

6.2.1 网络侧物理接口

AP北向接口应有1个10/100/1000 Base-T以太网接口或1个千兆光口，应符合GB/T 15629.3—2014标准，并且应支持采用直连网线进行连接，应支持自动校验连接网线的功能。

6.2.2 用户侧物理接口

AP 南向接口主要包含串口、无线等接口，各专业接口标准要求如下：

- a) 以太网接口：可选支持 1 个 100/1000 Base-T 以太网接口，应符合 GB/T 15629.3—2014 标准，并且应支持采用直连网线进行连接，应支持自动校验连接网线的功能；
- b) 无线接口：应符合 GB 15629.11、GB 15629.1102、GB 15629.1104、GB 15629.1101、T/WAPIA 007.1（含 XG1）、T/WAPIA 007.8、T/WAPIA 007.10 的规定，通过第三方权威检测机构检测，获得 WAPI 相关完整检测报告；
- c) 串口：应具备 1 个 RJ45 串口，不具备 RJ45 串口的 AP 应通过提供转接线、USB 等方式实现。

6.3 功能要求

6.3.1 IP 协议支持能力

AP 应支持 IPv4 和 IPv6 双栈协议，具备同时获取 IPv4 和 IPv6 地址的能力，具体要求如下：

- a) 支持同时建立业务类型、绑定关系都一致的 IPv4、IPv6 两条路由网络连接，两条连接分别获取 IPv4、IPv6 的地址，分别支持 IPv4 和 IPv6 的应用，并能够同时生效；
- b) 支持建立一条支持 IPv4、IPv6 双栈的网络连接，同时获取 IPv4、IPv6 的地址，同时支持 IPv4 和 IPv6 的应用；
- c) 能够根据获取 IP 地址的类型，自动启用相应的协议栈；对于同时获取到 IPv4/IPv6 地址的情况，优选使用 IPv6 地址；
- d) 访问外网时，能够根据外网目的 IP 地址的类型，自动启用相应的协议栈进行外网访问；若外网目的地址 IPv4、IPv6 同时存在，优选使用 IPv6 地址；
- e) IPv6 协议可以由后台管控系统进行远程开启或关闭；
- f) 在启用 IPv4、IPv6 双栈协议时，根据用户数据的协议（IPv4 或 IPv6）进行同协议类型的路由转发。

6.3.2 IPv4 功能

本项要求包括：

- a) 面向网络侧，应支持静态配置 IP 地址、DHCP 两种工作方式，遵循 RFC 2131 标准；
- b) 可支持基于终端设备类型分配同一地址段的不同区间的 IP 地址，并根据设备类型开放所需的协议端口，要求设备类型和地址区间的对应关系可以配置；
- c) 根据设备发现配置 IP 地址及开放的协议端口。

6.3.3 IPv6 功能

本项要求包括：

- a) 设备应支持 SLAAC 和 DHCPv6 服务器，可为 STA 设备公告 IPv6 地址前缀；
- b) 网络侧 IPv6 地址前缀可通过 SLAAC 获取，即自动向网络侧路由器请求地址前缀，并根据下发的前缀生成 IPv6 全局地址。

6.3.4 AC 发现方式

AP 应支持如下 AC 发现方式：手动配置，二层发现，DHCP OPTION 43（IPv4）/DHCP OPTION 52（IPv6），通过 DNS 域名解析发现等。

6.3.5 业务转发方式

AP 应支持业务本地转发方式，宜支持业务集中转发方式。

6.3.6 漫游切换支持能力

AP 应支持漫游切换，切换中保证业务不间断。

6.3.7 功率控制

本项要求包括：

- a) AP 应支持固定功率调整；
- b) AP 应支持自适应功率动态调整以降低干扰；
- c) 自动功率调整不影响已有的业务连接。

6.3.8 接入控制

本项要求包括：

a) 简单接入控制能力

- 1) AP 应支持基于 SSID 的接入控制；
- 2) AP 应支持基于 MAC 地址的接入控制；
- 3) AP 可支持基于终端操作系统的接入控制。

b) 限制最大关联用户数

为保证 WLAN 网络的连接服务质量，AP 应当具有限制最大关联用户数的功能、基于 SSID 的用户数限制功能。

c) 多 SSID 能力

AP 应支持多 SSID 功能，应支持 8 个，宜支持 16 个，支持多 SSID 之间的隔离，能够为不同 SSID 配置不同的 VLAN。

6.3.9 用户隔离功能

AP 应支持单 AP 及不同 AP 下的二层隔离功能；支持用户隔离功能的打开和关闭；宜默认打开二层隔离功能。

6.3.10 VLAN 支持能力

AP 应支持 IEEE 802.1Q 的 VLAN，支持对同一个 AP 下用户不同 VLAN 的分配和标记能力：

- a) 支持根据用户接入的 SSID 等方式划分 VLAN；
- b) 上行以太网口应支持 VLAN Trunk 功能；
- c) 应支持同一个 VLAN 中不同的无线用户之间的访问隔离。

6.3.11 QoS 支持能力

AP 应支持 WLAN QoS 功能要求。

6.3.12 WLAN 功能

AP 应具备 WLAN 功能，具体功能要求如下：

- a) 应支持 WLAN 功能启用和禁用，默认为启用；
- b) 应支持 SSID 中文编码和英文编码，中文编码应符合 GB 18030，英文编码应符合 GB/T 1988；
- c) 应支持 50 ms~1000 ms 内的某一信标帧间隔；
- d) 应支持自动速率调节，可选支持手工配置方式；
- e) 应支持 STA 在节电模式下工作，能够识别 STA 进入节电状态，并缓存相关数据；并支持 STA 在节电模式与非节电模式之间的动态切换；
- f) 应支持自动信道选择和手工配置两种方式，默认自动信道选择方式；
- g) 应支持发射功率可调，发射功率等技术参数符合我国无线电管理政策法规相关要求；
- h) 应支持同一个 VLAN 中不同的无线终端之间的访问隔离；
- i) 应支持 11a/b/g/n/ac 工作模式，宜支持 11ax 工作模式；
- j) 宜支持接收分段报文；
- k) 可选支持内置天线和外置天线方式。

6.4 安全要求

6.4.1 网络侧安全

本项要求宜由 AP 与 AC 配合提供，具体包括：

- a) 应支持对用户的基于 MAC 地址、IP 地址和 IP 地址范围等的 ACL 功能；
- b) 应支持 IP 报文过滤功能，可选支持应用层报文过滤；
- c) 宜提供一定的防 DoS 攻击能力，例如，能够防止 LAND、Ping of Death、SYN Flooding、ICMP Redirection、Smurf、Winnuke 等类型的攻击；
- d) 宜提供防端口扫描功能；

- e) 宜提供防非法报文攻击能力。

6.4.2 空口安全

本项要求包括：

- a) 应支持配置不同 SSID 以区分网络，支持 SSID 广播开启/关闭功能，默认关闭此功能；
- b) 应支持 WAPI 安全机制，符合 GB 15629.11—2003 和 GB 15629.11—2003/XG1—2006 标准的规定，支持国家密码管理主管部门批准的用于无线局域网的算法；
 - 1) 支持密钥更新功能，包括单播密钥更新、组播密钥更新和基密钥更新；
 - 2) WAPI-Cert 工作模式下，应支持 GB/T 16264.8—2005 中规定的 X.509 v3 证书，证书格式包括 PEM (X.509)、PKCS#12 (X.509)；
 - 3) WAPI-PSK 工作模式下，应支持手工设置预共享密钥，预共享密钥应支持 ASCII 码和十六进制两种输入方式。
 - 4) 可支持 AP 产生 WAPI 公私钥对并生成证书申请文件（符合 PKCS#10 证书请求标准），证书私钥数据以受保护方式进行存储，包括加密存储或专用硬件模块等方式。
- c) 对错误帧和空数据帧的处理
 - 1) 应能解析所接收 MAC 帧帧头中的各个字段；当所接收 MAC 帧帧头中含有错误或不可识别信息时，应能丢弃该帧；应能忽略未知类型的信息元素；
 - 2) 在收到空数据帧后应能正常工作；从一个未链路验证或未关联的 STA 收到空数据帧的时候，应能解除链路验证或解除关联。
- d) 支持强制 STA 下线功能；
- e) 支持否定非法证书功能；
- f) 支持 MAC 地址过滤功能；
- g) 宜支持与后台系统配合，切断非法 STA 的网络连接。

6.5 管理和维护要求

6.5.1 基本要求

AP 应支持本地管理和远程管理。

6.5.2 日志要求

AP 应支持上传日志记录，含外部攻击记录、告警信息记录等。

6.5.3 配置文件备份

配置文件应具备如 CRC 校验码、MD5 校验码等方式进行合法性校验，配置文件更新时应同时更新两个配置文件，读取配置时应使用如 CRC、MD5 等方式校验合法的那个配置文件。

6.5.4 系统信息管理

本项要求包括：

- a) 设备状态
设备状态显示 AP 的总体设备信息和工作状态：
 - 1) 设备信息：宜包含设备型号、设备标识号、硬件版本、软件版本；
 - 2) 网络侧连接信息：显示网络侧连接状态、IP 地址、子网掩码、默认网关、DNS 服务器等；
 - 3) 用户侧接口信息：
WLAN 接口信息：仅显示用户个性化 SSID 的 WLAN 的连接状态、SSID、信道、加密状态信息；
以太网接口信息：显示 IP 地址、MAC 地址、收发包数；
 - 4) 远程管理状态（仅提供给网络维护人员）
远程管理状态显示 AP 的如远程连接建立状态、业务下发状态等信息。
- b) 设备日志
显示管理配置操作记录、外部攻击记录、告警信息记录等。

6.5.5 设备管理

本项要求包括：

- a) 管理员管理：
 - 1) 支持默认账号的默认密码修改；
 - 2) 可支持添加管理员账号，支持对添加管理员账号的删除或停用；
 - 3) 支持管理员账号的密码验证后修改；
 - 4) 支持管理员分权管理。
- b) 日志文件管理
应支持日志文件写入等级设置，只有日志等级高于此限制的信息才记入到日志文件。
- c) 软件、固件升级
AP 软件、固件可提供 Web、SNMP 等方式进行本地升级或远程升级。
- d) 应支持设备重启；
- e) 应支持通过手动按键等方式恢复出厂设置。

6.5.6 网络诊断

支持网络诊断，如ping测试等，根据管理员分级管理的要求，仅网络维护人员具有网络诊断操作权限。

6.5.7 身份鉴别

本项要求包括：

- a) 应支持对登录 AP 的管理员进行身份标识和鉴别，身份标识具有唯一性；
- b) 应具有登录失败处理功能，应具备限制非法登录次数和当登录连接超时自动退出等功能；
- c) 当进行远程管理时，应使用安全的远程登录的协议。

6.6 性能要求

6.6.1 用户容量

当AP和WLAN终端在无阻挡的传播环境中WAPI安全方式下用户容量应达到如下要求：

- a) GB 15629.1102（11b）模式，用户容量要求见下：
平均每用户单向吞吐量 ≥ 200 kbps，同时工作用户数 ≥ 10 个。
- b) GB 15629.1104（11g）模式，用户容量要求见下：
 - 1) 平均每用户单向吞吐量 ≥ 300 kbps，同时工作用户数 ≥ 30 个；
 - 2) 平均每用户单向吞吐量 ≥ 500 kbps，同时工作用户数 ≥ 15 个，同时关联用户数为 64 个。
- c) GB 15629.1101（11a）模式，用户容量要求见下：
 - 1) 平均每用户单向吞吐量 ≥ 300 kbps，同时工作用户数 ≥ 30 个；
 - 2) 平均每用户单向吞吐量 ≥ 500 kbps，同时工作用户数 ≥ 15 个，同时关联用户数为 64 个。
- d) 11n/ac/ax 模式，用户容量要求见表 1。

表1 11n/ac/ax 模式用户容量要求

工作模式	空间流	频宽模式	平均每用户上行/ 下行吞吐量	用户容量	
				同时工作用户数	同时关联用户数
11n模式	一条空间流	HT20	≥ 500 kbps	≥ 25 个	/
		HT40	≥ 1 Mbps	≥ 25 个	/
	二条空间流	HT20	≥ 1 Mbps	≥ 25 个	/
		HT40	≥ 1.5 Mbps	≥ 25 个	64个
	三条空间流	HT20	≥ 1.5 Mbps	≥ 25 个	/
		HT40	≥ 2 Mbps	≥ 25 个	64个
	四条空间流	HT20	≥ 3 Mbps	≥ 25 个	/

表1 11n/ac/ax 模式用户容量要求 (续)

工作模式	空间流	频宽模式	平均每用户上行/ 下行吞吐量	用户容量	
				同时工作用户数	同时关联用户数
11ac模式	一条空间流	HT40	≥ 4 Mbps	≥ 25 个	64个
		VHT20	≥ 1 Mbps	≥ 25 个	/
		VHT40	≥ 2 Mbps	≥ 25 个	64个
		VHT80	≥ 4 Mbps	≥ 25 个	64个
	二条空间流	VHT20	≥ 2 Mbps	≥ 25 个	/
11ac模式	二条空间流	VHT40	≥ 4 Mbps	≥ 25 个	64个
		VHT80	≥ 8 Mbps	≥ 25 个	64个
	三条空间流	VHT20	≥ 3 Mbps	≥ 25 个	/
		VHT40	≥ 6 Mbps	≥ 25 个	64个
		VHT80	≥ 12 Mbps	≥ 25 个	64个
	四条空间流	VHT20	≥ 4 Mbps	≥ 25 个	/
		VHT40	≥ 8 Mbps	≥ 25 个	64个
		VHT80	≥ 16 Mbps	≥ 25 个	64个
	11ax模式	一条空间流	HE20	≥ 1.5 Mbps	≥ 30 个
			HE40	≥ 3 Mbps	≥ 30 个
			HE80	≥ 4 Mbps	≥ 30 个
	二条空间流	HE20	≥ 3 Mbps	≥ 30 个	/
		HE40	≥ 6 Mbps	≥ 30 个	64个
		HE80	≥ 8 Mbps	≥ 30 个	64个
	三条空间流	HE20	≥ 4.5 Mbps	≥ 30 个	/
		HE40	≥ 8 Mbps	≥ 30 个	64个
		HE80	≥ 12 Mbps	≥ 30 个	64个
	四条空间流	HE20	≥ 6 Mbps	≥ 30 个	/
		HE40	≥ 12 Mbps	≥ 30 个	64个
		HE80	≥ 16 Mbps	≥ 30 个	64个

6.6.2 吞吐量

当AP覆盖的范围内仅有1个终端,且为室内外AP和WLAN终端无阻挡的传播环境中WAPI安全方式下系统吞吐量应达到如下要求:

- 在GB 15629.1102 (11b) 模式下,上下行吞吐量 ≥ 4.5 Mbps;
- 在GB 15629.1104 (11g) 模式下,上下行吞吐量 ≥ 18 Mbps;
- 在GB 15629.1101 (11a) 模式下,上下行吞吐量 ≥ 18 Mbps;
- 在11n/ac/ax模式下,上下行吞吐量要求见表2。

表2 11n/ac/ax 模式吞吐量要求

工作模式	空间流	频宽模式	上下行吞吐量
11n模式	一条空间流	HT20	≥ 32 Mbps
		HT40	≥ 60 Mbps
	二条空间流	HT20	≥ 64 Mbps
		HT40	≥ 120 Mbps

表2 11n/ac/ax 模式吞吐量要求（续）

工作组模式	空间流	频宽模式	上下行吞吐量
	三条空间流	HT20	≥ 96 Mbps
		HT40	≥ 180 Mbps
	四条空间流	HT20	≥ 128 Mbps
		HT40	≥ 240 Mbps
11ac模式	一条空间流	VHT20	≥ 36 Mbps
		VHT40	≥ 64 Mbps
		VHT80	≥ 150 Mbps
11ac模式	二条空间流	VHT20	≥ 72 Mbps
		VHT40	≥ 128 Mbps
		VHT80	≥ 300 Mbps
	三条空间流	VHT20	≥ 108 Mbps
		VHT40	≥ 192 Mbps
		VHT80	≥ 360 Mbps
	四条空间流	VHT20	≥ 144 Mbps
		VHT40	≥ 256 Mbps
		VHT80	≥ 480 Mbps
11ax模式	一条空间流	HE20	≥ 48 Mbps
		HE40	≥ 97 Mbps
		HE80	≥ 180 Mbps
	二条空间流	HE20	≥ 97 Mbps
		HE40	≥ 195 Mbps
		HE80	≥ 360 Mbps
	三条空间流	HE20	≥ 144 Mbps
		HE40	≥ 390 Mbps
		HE80	≥ 540 Mbps
	四条空间流	HE20	≥ 195 Mbps
		HE40	≥ 392 Mbps
		HE80	≥ 720 Mbps

6.6.3 时延

AP在WAPI安全方式下传输时的单向时延不大于50 ms。

6.6.4 抖动

AP在WAPI安全方式下传输时的最大抖动不大于50 ms。

6.6.5 丢包率

AP在WAPI安全方式下传输时的丢包率不大于1%。

6.6.6 接收灵敏度

AP的接收灵敏度应符合YD/T 3168相关要求。

6.6.7 可靠性

采用MTBF衡量AP可靠性水平，AP的m1值（MTBF的不可接受值）不应低于10 000 h。

6.6.8 其它要求

本项要求包括：

- a) 整机功率 ≤ 55 W;
- b) 应具备双射频, AP 每射频最大可接入用户数或终端数 ≥ 64 个;
- c) MAC 地址学习数量应 ≥ 64 个;
- d) AP 的 WLAN 覆盖能力, 室内宜采用全向天线, 室外采用全向或定向天线。

6.7 运行环境要求

6.7.1 工作温度

室内型: $0\text{ }^{\circ}\text{C} \sim 45\text{ }^{\circ}\text{C}$ 。

室外型: $-15\text{ }^{\circ}\text{C} \sim 55\text{ }^{\circ}\text{C}$ 。

6.7.2 存储温度

室内外均为 $-40\text{ }^{\circ}\text{C} \sim 55\text{ }^{\circ}\text{C}$ 。

6.7.3 工作湿度

室内外均为 $10\% \sim 95\%$ RH不凝结。

6.7.4 存储湿度

室内外均为 $10\% \sim 95\%$ RH不凝结。

6.7.5 防尘防水等级

室外型: 应满足GB/T 4208标准中定义的IP66等级, 可选IP67、IP68等级。

6.7.6 大气压

应能在以下大气压条件下的环境中正常工作: $86\text{ kPa} \sim 106\text{ kPa}$ 。

6.7.7 抗风强度

室外型: 满足抗风强度: ≥ 90 MPH (应承受12级台风)。

6.7.8 机械环境适应性

机械环境适应性应符合表3~表7的规定。

表3 正弦振动适应性

试验项目	试验内容	参数
初始和最后振动响应检查	频率范围 Hz	5~200
	扫频速度 oct/min	≤ 1
	驱动振幅 mm	0.15
	驱动振幅 mm	0.15
	持续时间 min	30 ± 1
扫频耐久试验	频率范围 Hz	5~200
	扫频速度 oct/min	≤ 1
	驱动振幅 mm	0.15
	循环次数	5

注: 振动测试使用正弦波形, 表中驱动振幅为峰值。

表4 随机振动适应性

振动谱型	总均方根加速度 m/s^2	振动方向	每方向振动时间 min
5 Hz~20 Hz, $0.02\text{g}^2/\text{Hz}$	6.9	3	5
20 Hz~500 Hz, -3 dB/oct	6.9	3	5

表5 冲击适应性

峰值加速度 m/s^2	脉冲持续时间 ms	冲击波形
300	11	半正弦波

表6 碰撞适应性

峰值加速度 m/s^2	脉冲持续时间 ms	碰撞次数	碰撞波形
150	11	1 000	半正弦波

表7 自由跌落适应性

跌落高度 mm	次数
250	六个方向，每个方向一次

6.7.9 接地

室外AP应支持接地端子，接地电阻不大于10欧姆时AP设备应能正常工作。

6.7.10 电磁兼容性

本项要求包括：

- AP的传导杂散骚扰应满足 YD/T 1312.2—2004 中 8.1 的限值要求；
- AP的辐射杂散骚扰应满足 YD/T 1312.2—2004 中 8.2 的限值要求；
- AP的连续骚扰应满足 YD/T 1312.2—2004 中 8.3、8.4、8.5、8.6 的限值要求；
- AP的谐波电流应满足 YD/T 1312.2—2004 中 8.7 的限值要求；
- AP的静电放电抗扰度应满足 YD/T 1312.2—2004 中 9.1 的限值要求；
- AP的辐射骚扰抗扰度应满足 YD/T 1312.2—2004 中 9.2 的限值要求；
- AP的电快速瞬变脉冲群抗扰度应满足 YD/T 1312.2—2004 中 9.3 的限值要求；
- AP的浪涌抗扰度应满足 YD/T 1312.2—2004 中 9.4 的限值要求；
- AP的射频场感应的传导骚扰抗扰度应满足 YD/T 1312.2—2004 中 9.5 的限值要求；
- AP的工频磁场抗扰度应满足 YD/T 1312.2—2004 中 9.6 的限值要求。

6.7.11 绝缘电阻

AP设备的绝缘电阻应不小于50 MΩ。

6.7.12 运行电气条件

本项要求按照以下a和（或）b和（或）c实现：

- 220 V（单相）波动范围：220 V±22 V，50 Hz±1 Hz；
- 48 V 直流：设备能够在下列供电变化范围内正常工作：-57 V~-40 V；
- PoE 供电模式下：支持 IEEE 802.3af 或 IEEE 802.3at 或 IEEE 802.3bt 以太网供电标准，使用 PoE 供电方式时，供电传输距离能力应不小于 60 米。

7 接入点控制器

7.1 基本要求

本项要求包括：

- AC 应支持双机热备份，故障切换时不影响业务正常运行，切换时间小于 500 ms；
- AC 设备可选支持风扇多级自动调速，可以通过检测周围环境自动调整风扇转速，降低能耗；
- AC 应支持双电源备份；
- AC 可支持 AC 集群部署，中心 AC 管理分布 AC 模式。

7.2 物理接口要求

AC 接口主要包含以太网接口、串口等接口，各接口标准要求如下。

- a) 支持 100/1000 Mbps 以太网接口;
- b) 支持 1000 BASE-X 以太网光接口;
- c) AC 设备网络侧接口可选支持 10 GE 光口;
- d) AC 对外应呈现统一接口, 不能由于扩容而增加或调整对外接口连线, 除非转发容量超过已连接端口容量;
- e) 宜支持调试串口, 便于调试维护;
- f) 应支持广域网接口, 如支持光口、以太网口等。

7.3 功能要求

7.3.1 路由功能

AC应支持IPv4和IPv6静态路由功能, 可选支持动态路由协议, 如RIP、OSPF等。

7.3.2 WAPI 功能

AC应支持WAPI功能, 终端应能够通过WAPI证书鉴别过程安全接入网络, 并获得AC通过DHCP分配的IP地址、通过授权。

可支持AC产生WAPI公私钥对并生成证书申请文件(符合PKCS#10 证书请求标准), 证书私钥数据以受保护方式进行存储, 包括加密存储或专用硬件模块等方式。

AC应能成功安装WAPI证书。

7.3.3 DHCP 功能

AC应实现DHCP服务器功能, 且应支持DHCP中继功能。AC的DHCP功能应符合RFC 2131的规定。

7.3.4 VLAN 功能

AC设备应具备VLAN功能, 满足如下要求:

- a) AC 应支持 VLAN Trunk 功能;
- b) AC 应支持 VLAN 终结特性, 在同一个三层接口下, 不同 VLAN 的用户可使用同一个地址池。

7.3.5 二层功能

AC应支持LACP。

AC应支持STP功能, 防止组网环路引起的广播风暴。

7.3.6 三层功能

AC应支持IPv4和IPv6双栈协议, 具备同时获取IPv4和IPv6地址的能力。

7.3.7 IPv4 支持能力

本项要求包括:

- a) AC 应支持 DHCP Server, 为瘦 AP 和无线终端动态分配 IP 地址的功能; 同一个 DHCP Server (同一个网段 IP 地址池) 应能同时为不同管理 VLAN (AP 上联设备发起的 VLAN, 终结到 AC) 的瘦 AP 和无线终端动态分配 IP 地址的能力;
- b) 要求 AC 整机设备公用一个 DHCP 地址池 (同网段), 也可支持多个 DHCP 地址池, 地址池的总容量应不小于 20 K;
- c) 应支持 DHCP Relay。

7.3.8 IPv6 支持能力

本项要求包括:

- a) AC 应支持 IPv6 协议栈, 包括 ICMPv6 等;
- b) AC 应支持 ND (Neighbor Discover) 协议, 并可在 RA 通告中通告终端通过 DHCP 方式获取 IPv6 地址;
- c) 应支持 SLAAC 和 DHCPv6 Server;
- d) 应支持 DHCPv6 Relay;
- e) 应支持 IPv6 隧道, AP 和 AC 支持通过 IPv6 地址建立隧道连接。

7.3.9 设备发现功能

AC应支持瘦AP对AC进行自动识别,包括:支持基于二层协议的发现方式、支持基于三层协议的发现方式。

7.3.10 业务转发

AC设备应支持集中转发和(或)本地转发的业务转发能力,包括IPv4和IPv6用户数据的集中转发和(或)本地转发。

集中转发模式下,可以充当网络出口的功能,NAC具备NAT功能,支持PPPoE拨号、静态IP、DHCP自动获取三种主流上网接入方式。

7.3.11 速率控制

AC应具备控制每个在线用户最大可用速率的功能。

7.3.12 强制下线

AC应具有强制在线用户下线的功能。

7.3.13 QoS 功能

本项要求包括:

- a) AC 应具备支持不同用户和业务的优先级能力;
- b) 支持二层 IEEE 802.1Q 和三层 DSCP QoS 之间的映射,保证高优先级业务流的质量。

7.3.14 管理 AP 功能

AC应能够对与其连接的AP设备进行管理,包括对AP进行参数配置、恢复出厂设置、重启以及升级等。

7.3.15 同步要求

AC应支持AP和AC间基于NTP的时间同步。

7.3.16 扩展要求

可选支持无线网络展开物联网应用,对能耗、环境、业务系统的物联网升级;对物联网设备管理及采集数据信息。

7.4 安全要求

7.4.1 接入控制

为了支持必要的风险控制功能,接入系统应根据管理系统的指令,中断状态异常用户的网络连接。

- a) 支持对用户的 MAC 地址、IP 地址、端口号等方面的接入控制列表 (ACL) 功能;
- b) 支持基于用户状态(网络侧下发)自动断开用户网络连接的功能;
- c) 支持基于后台管理系统下发的断开消息实时断开用户网络连接;
- d) 支持用户的连接时长控制。

7.4.2 网络访问安全

- a) AC 应支持基于 MAC 地址的接入控制,包括黑名单和白名单;
- b) AC 应支持 WAPI 鉴别;
- c) 可支持多因素结合认证,保证网络的安全性。

7.4.3 二层隔离要求

应支持单个AP及不同AP下的二层隔离功能;应支持用户隔离功能的打开和关闭。

7.4.4 WLAN 防非法攻击能力

本项要求包括:

- a) 应支持白名单功能,指定允许接入的终端列表;
- b) 应支持黑名单功能,指定不允许接入的终端列表。

7.4.5 非法 AP 检测

为了防止非法AP对合法AP的信号传输产生干扰,甚至欺骗合法用户,骗取用户的注册信息,WLAN接入系统应该具有非法AP检测的功能,并能在有条件的情况下,通过与后台系统配合,切断非法AP的网络连接。

7.4.6 防止假冒能力

应支持同时基于MAC地址、IP地址、以及网络侧信息（如VLAN ID等）的捆绑来识别用户，防假冒的实现不能影响合法用户的漫游及业务使用。

7.4.7 防 DoS 攻击能力

AC应支持防DoS攻击能力。

7.4.8 用户地址核查

本项要求包括：

- a) 应支持核查用户地址与 DHCP 地址池，非 DHCP 地址池下发的地址不予转发；
- b) DHCP 过程中需首先核查用户 MAC 地址是否有对应的尚在租期内的 IP 地址，如有则给用户分配相同的 IP 地址而非新的 IP 地址；
- c) 可支持核查用户数据包的源 IP 地址，若源 IP 地址非法则不予转发，例如源 IP 地址与 VLAN 不匹配，与 MAC 不匹配，与 SSID 不匹配或不在合法的源地址池等。

7.5 管理和维护要求

7.5.1 操作维护功能

AC应支持Console管理、WEB管理、Telnet管理、SNMP管理中的一种或几种，并应支持安全管理功能；Telnet管理功能应默认关闭。

7.5.2 网管功能

本项要求包括：

- a) 支持标准和开放的网络管理接口，应支持 SNMP（v2c 或以上版本）、FTP、Telnet、SSH；
- b) 支持标准和开放的管理信息库，可支持 MIB II、802.3 MIB、GB 15629.11 MIB 等。

7.5.3 日志要求

AC支持日志记录及输出功能：对AP接入、用户接入、地址分配、用户认证、无线安全事件等相关重要信息具备分级日志记录及输出功能。

7.5.4 远程故障诊断

AC 应能配合实现如下的远程故障诊断功：

- a) AP 远程复位重启；
- b) AC 实时监控 AP 的工作状态，AP 下线要通知网络管理系统。

7.5.5 设备管理

本项要求包括：

- a) 管理员管理：
 - 1) 支持默认账号的默认密码修改；
 - 2) 可支持添加管理员账号，支持对添加管理员账号的删除或停用；
 - 3) 支持管理员账号的密码验证后修改；
 - 4) 支持管理员的分权分级管理。
- b) 应支持设备重启；
- c) 应支持恢复设备出厂设置；
- d) 可支持对接入的无线终端信息可视化，例如：上网时长、终端类型、接收速率、发送速率、信号强度、射频接入、网络接入、认证类型等。

7.5.6 身份鉴别

本项要求包括：

- a) 应支持对登录 AC 的管理员进行身份标识和鉴别，身份标识具有唯一性；
- b) 应具有登录失败处理功能，应具备限制非法登录次数和当登录连接超时自动退出等功能；
- c) 当进行远程管理时，应使用安全的远程登录的协议。

7.5.7 安全审计

本项要求包括：

- a) 应支持安全审计功能；
- b) 支持本地转发五元组审计，审计的内容包括源 IP 地址，源端口，目的 IP 地址，目的端口和传输层协议；
- c) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
- d) 应支持审计记录备份功能；
- e) 可选支持审计功能与公安网监平台对接。

7.6 性能要求

7.6.1 吞吐量

AC的吞吐量要求不小于2 Gbps，对于1024个AP模型配置的AC设备满配要求不小于10 Gbps，对于2048个AP模型配置的AC设备满配要求不小于50 Gbps，对于4096个AP模型配置的AC设备满配要求不小于100 Gbps，宜满足40 Mbps×AC最大支持的AP数。

7.6.2 无线控制

本项要求包括：

- a) AC 应支持同时工作的无线终端数应不小于 4 K 用户，宜满足 20×AC 最大支持的 AP 数；
- b) AC 设备支持的 MAC 地址数量应不小于 8 K，宜满足 40×AC 最大支持的 AP 数；
- c) AC 设备支持的 ACL 数目应不小于 2 K，宜满足 20*AC 最大支持的 AP 数；
- d) AC 转发时延小于 50 us，不丢包。

7.6.3 接入控制

DHCP的处理性能：

- a) 对应于 1024 个 AP 模型配置的 AC 设备：
 - 1) 整机本地地址池数量要求不小于 96 个；
 - 2) 整机本地地址池分配的地址总数量不小于 96*256；
- b) 对应于 2048 个 AP 模型配置的 AC 设备：
 - 1) 整机本地地址池数量要求不小于 128 个；
 - 2) 整机本地地址池分配的地址总数量不小于 128*256；
- c) 对应于 4096 个 AP 模型配置的 AC 设备：
 - 1) 整机本地地址池数量要求不小于 1024 个；
 - 2) 整机本地地址池分配的地址总数量不小于 1024*256。

7.6.4 稳定性

AC应能支持包长为64字节、128字节、256字节、512字节、1024字节、1280字节、1518字节的数据的12 h连续稳定传输。

7.6.5 可靠性

采用MTBF衡量AC可靠性水平，AC的m1值（MTBF的不可接受值）不应低于10 000 h。

7.6.6 可用性

AC设备的年可用性指标为99.999%。

7.7 运行环境要求

7.7.1 工作温度

10℃～35℃。

7.7.2 存储温度

-40℃～55℃。

7.7.3 工作湿度

10%～95% RH不凝结。

7.7.4 存储湿度

10%~95% RH不凝结。

7.7.5 大气压

应能在以下大气压条件下的环境中正常工作：86 kPa~106 kPa。

7.7.6 电磁兼容性

本项要求包括：

- a) AC 的无线电骚扰应符合 GB/T 9254 中对 A 级限值规定；
- b) AC 的谐波电流应符合 GB/T 17625.1 中对 D 类限值要求；
- c) AC 的抗扰度应符合 GB/T 17618 的规定。

7.7.7 运行电气条件

本项要求按照以下a)和（或）b）实现：

- a) 220 V（单相）波动范围：220 V±22 V，50 Hz±1 Hz；
- b) -48 V 直流：设备能够在下列供电变化范围内正常工作：-40 V~57 V。

8 鉴别服务器

8.1 基本要求

本项要求包括：

- a) 支持 WAPI 协议；
- b) AS 应支持 1:1 热备份或 N+1 备份，故障切换时不影响业务正常运行，切换时间小于 500 ms；
- c) AS 设备可选支持风扇多级自动调速，可以通过检测周围环境自动调整风扇转速，降低能耗；
- d) 支持双电源备份。

8.2 物理接口要求

本项要求包括：

- a) 以太网接口：应有 1 个 10/100/1000 Base-T 以太网接口，应符合 GB/T 15629.3—2014 标准，并且应支持采用直连网线进行连接，应支持自动校验连接网线的功能。可选支持 1 个或以上个千兆光口；
- b) 串口：应具备 1 个 RJ45 串口；
- c) USB 接口：应具备 1 个 USB 接口，满足 USB 2.0 协议标准要求。

8.3 功能要求

8.3.1 协议流程和数据格式

AS应支持WAPI证书鉴别协议流程，应能成功安装WAPI证书，鉴别协议流程和数据格式应符合GB 15629.11—2003和GB 15629.11—2003/XG1—2006标准的规定，能够接收AP的证书鉴别请求分组，向AP返回证书鉴别响应分组。

8.3.2 设备信息管理

管理员登录管理端后，进入设备信息管理功能页面，可以分别对STA和AP进行信息管理，包括STA和AP的设备信息包括MAC地址信息、设备证书信息等，可以实现设备的增删改查操作。

8.3.3 证书管理

管理员通过登录管理端后，进入业务管理功能页面，可以对STA和AP证书进行管理，包括申请、审核、下载等管理操作。

8.3.4 授权管理

管理员可以将设备添加到创建的组，并进行增删改查操作，可以基于组创建授权策略。也可以直接为STA或AP设备进行授权。

8.3.5 证书鉴别

本项要求包括：

- a) 终端用户使用证书访问无线局域网，AP 和 STA 通过 AS 对对方证书进行鉴别，鉴别通过后终端

设备才可接入无线网络；

- b) AS 应支持绑定证书信息和 MAC 地址的终端通过鉴别，支持拒绝错误绑定证书信息和 MAC 地址的终端通过鉴别。

8.3.6 CIS 证书同步

支持与CIS的数据同步功能，可接收CIS下发的密钥、证书和CRL，并安全存储。

8.3.7 与 CIS 安全通信功能

AS与CIS之间涉及证书、密钥等的通信应进行安全保护，可使用GM/T 0014相关协议。

8.3.8 CRL 验证

支持CRL验证功能，对于在CRL中的证书，禁止该设备通过验证。

8.3.9 漫游功能

AS应支持根据证书持有者身份信息在本地AS和信任AS之间执行证书漫游鉴别，符合T/WAPIA 010.2-2010标准。

8.3.10 端口号

AS处理WAPI鉴别数据报文的UDP端口号应符合GB 15629.11—2003/XG1—2006标准规定。

8.3.11 数据备份和恢复

AS应有数据备份和恢复策略，能够实现数据的备份与恢复。

8.4 安全要求

8.4.1 系统要求

AS所使用的操作系统应进行安全加固，裁减一切不需要的模块，关闭所有不需要的端口和服务，仅开放UDP 3810及其他所需端口。

8.4.2 密码算法

AS应支持国家密码管理主管部门批准的用于无线局域网的算法。

8.4.3 证书及密钥管理

AS应对自身密钥和证书安全存储和管理，防止密钥被窃取、拷贝；应对签发过的AP和STA证书做好存储和管理，防止信息泄露。

8.4.4 安全管理

AS应设置管理员，满足相应管理权限可进行管理操作。对管理操作具备日志审计功能。

8.4.5 物理安全防护

AS在设计、硬件配置等方面要采取相应的保护措施，保证设备基本的物理安全防护功能。

8.5 管理和维护要求

8.5.1 管理员管理

本项要求包括：

- a) 应提供出厂设备管理员凭证，并可在管理界面增加或删除管理员；
- b) 管理员凭证应采用USB-KEY数字证书方式，确保AS的安全登录和安全管理。

8.5.2 日志要求

本项要求包括：

- a) 日志应记录事件发生的时间、事件的操作者、操作类型及操作结果等信息；
- b) 应能按时间、操作者、操作类型等对日志进行分类或综合查询。

8.5.3 安全审计

应提供审计管理的接口/界面，能够对事件发生的时间、事件的操作者、操作类型及操作结果等信息进行审计。

8.6 性能要求

8.6.1 鉴别性能

AS应支持多用户鉴别，鉴别数量不低于500有效证书每秒。

8.6.2 可靠性

采用MTBF衡量AS可靠性水平，AS的m1值（MTBF的不可接受值）不应低于10 000 h。

8.6.3 可用性

AS设备的年可用性指标为99.99%。

8.7 运行环境要求

8.7.1 工作温度

10℃～35℃。

8.7.2 存储温度

-40℃～55℃。

8.7.3 工作湿度

10%～95% RH不凝结。

8.7.4 存储湿度

10%～95% RH不凝结。

8.7.5 大气压

应能在以下大气压条件下的环境中正常工作：86 kPa～106 kPa。

8.7.6 电磁兼容性

本项要求包括：

- a) AS的无线电骚扰应符合GB/T 9254中对A级限值要求；
- b) AS的谐波电流应符合GB/T 17625.1中对D类限值要求；
- c) AS的抗扰度应符合GB/T 17618的规定。

8.7.7 运行电气条件

电压220V（单相）波动范围：220 V±22 V，50 Hz±1 Hz。

9 证书签发服务器

9.1 基本要求

本项要求包括：

- a) CIS应支持1:1备份，故障倒换时不影响业务正常运行；
- b) 支持双电源备份。

9.2 物理接口要求

本项要求包括：

- a) 以太网接口：应有1个10/100/1000 Base-T以太网接口，应符合GB/T 15629.3—2014标准，并且应支持采用直连网线进行连接，应支持自动校验连接网线的功能。可选支持1个或以上个千兆光口；
- b) 串口：应具备1个RJ45串口；
- c) USB接口：应具备1个USB接口，满足USB 2.0协议标准要求。

9.3 功能要求

9.3.1 证书签发

本项要求包括：

- a) CIS应支持对证书的签发操作，包括能生成与签发证书，并支持证书的查询和下载；
- b) 数字证书应用采用国家密码管理主管部门批准的用于无线局域网的算法；
- c) CIS应支持将STA或AP的证书信息和STA或AP的MAC地址进行绑定。

9.3.2 CRL签发

CIS应根据CRL签发策略签发CRL文件，并支持CRL查询和下载。

9.3.3 证书更新

CIS应能为已注册的用户重新签发证书。

9.3.4 证书查询功能

CIS应支持按证书序列号对证书的查询，支持按证书持有者名称对证书的查询。

9.3.5 证书吊销功能

CIS应支持证书的吊销操作，支持按证书持有者名称等方式对证书的吊销，以及批量吊销，可支持签发CRL和LDAP协议。

9.3.6 证书状态查询

CIS应能提供实时证书状态查询服务。

9.3.7 设备信息管理

管理员登录管理端后，进入设备管理功能页面，可以分别对AS、STA和AP进行信息管理，包括AS、STA和AP的设备信息、MAC地址信息等，可以实现设备的增删改查操作。

9.3.8 授权管理

管理员登录管理端后，可进行设备分组管理，实现设备分组的增删改查操作，可以基于组创建授权策略。也可以直接为STA或AP设备进行授权。

9.3.9 统计分析功能

本项要求包括：

- a) 可对签发证书情况进行统计分析，包括已签发、待签发、已更新、已吊销等；
- b) 可按照设备类型进行证书签发统计。

9.3.10 数据备份和恢复

CIS应有数据备份和恢复策略，能够实现数据的备份与恢复。

9.3.11 与 AS 安全通信功能

CIS与AS之间涉及证书、密钥等的通信应进行安全保护，可使用GM/T 0014相关协议。

9.4 安全要求

9.4.1 系统要求

CIS所使用的操作系统应进行安全加固，裁减一切不需要的模块，关闭所有不需要的端口和服务。

9.4.2 密码算法

CIS应支持国家密码管理主管部门批准的用于无线局域网的算法。

9.4.3 安全管理

CIS应设置管理员，满足相应管理权限可进行管理操作。对管理操作具备日志审计功能。

9.4.4 物理安全防护

CIS在设计、硬件配置等方面要采取相应的保护措施，保证设备基本的物理安全防护功能。

9.5 管理和维护要求

9.5.1 管理员管理

本项要求包括：

- a) 应提供系统初始化管理员凭证，并可在管理界面增加或删除管理员；
- b) 管理员凭证应采用USB-KEY数字证书方式，确保CIS的安全登录和安全管理。

9.5.2 日志要求

本项要求包括：

- a) 日志应记录事件发生的时间、事件的操作者、操作类型及操作结果等信息；
- b) 应能按时间、操作者、操作类型等对日志进行分类或综合查询。

9.5.3 安全审计

应提供审计管理的界面，能够对事件发生的时间、事件的操作者、操作类型及操作结果等信息进行审计；

9.6 性能要求

9.6.1 证书容量

CIS应支持签发的有效证书数量不低于5000张。

9.6.2 可靠性

采用MTBF衡量CIS可靠性水平，CIS的m1值（MTBF的不可接受值）不应低于10 000 h。

9.6.3 可用性

CIS设备的年可用性指标为99.99%。

9.7 运行环境要求

9.7.1 工作温度

10℃~35℃。

9.7.2 存储温度

-40℃~55℃。

9.7.3 工作湿度

10%~95% RH不凝结。

9.7.4 存储湿度

10%~95% RH不凝结。

9.7.5 大气压

应能在以下大气压条件下的环境中正常工作：86 kPa~106 kPa。

9.7.6 电磁兼容性

本项要求包括：

- a) CIS的无线电骚扰应符合GB/T 9254中对A级限值要求；
- b) CIS的谐波电流应符合GB/T 17625.1中对D类限值要求；
- c) CIS的抗扰度应符合GB/T 17618的规定。

9.7.7 运行电气条件

220 V（单相）波动范围：220 V±22 V，50 Hz±1 Hz。

10 终端

10.1 基本要求

本项要求包括：

- a) 终端与AP之间的空中接口物理层应符合GB 15629.11—2003、GB 15629.1102—2003、GB 15629.1104—2006、GB 15629.1101—2006国家标准和T/WAPIA 007.1—2010、T/WAPIA 007.1—2010/XG1—2014、T/WAPIA 007.8—2016、T/WAPIA 007.10—2020、团体标准；
- b) 工作在2.4 GHz频段的终端的工作频率范围为2400 MHz~2483.5 MHz；
- c) 工作在5 GHz频段的终端的工作频率范围为5150 MHz~5350 MHz和5725 MHz~5850 MHz；
- d) 终端应获得国家无线电主管部门颁发的型号核准证书。

10.2 物理接口要求

本项要求包括：

- a) 无线接口：应符合GB 15629.11、GB 15629.1102、GB 15629.1104、GB 15629.1101、T/WAPIA 007.1（含XG1）、T/WAPIA 007.8、T/WAPIA 007.10的规定，通过第三方权威检测机构检测，获得WAPI相关完整检测报告；
- b) CPE可选支持1个10/100/1000 Base-T以太网接口，接口支持PoE供电方式，符合GB/T 15629.3—2014标准；
- c) CPE可选支持1个RS232和RS485数据采集接口，接口支持ModBus协议。

10.3 功能要求

10.3.1 扫描AP功能

终端应支持AP扫描功能，能够搜索到周围无线环境中存在的AP设备。

10.3.2 SSID 配置

终端可选支持对SSID的设置，并与对应的AP设备建立关联。

10.3.3 分段门限设置

终端可选支持对分段门限的设置。

10.3.4 RTS 门限设置

终端可选支持对RTS门限的设置。

10.3.5 节能功能

终端应支持节能功能。

10.3.6 安全功能

本项要求包括：

a) 证书安装

终端应能成功安装WAPI证书。

b) 证书选择功能

终端应优先选择使用和本地AP具有相同AS的证书；如果没有安装和本地AP具有相同AS的证书，应能发起接入鉴别请求，其中包含STA现有证书。

c) 证书鉴别功能

终端应能实现完整的WAI鉴别流程，并在成功完成WAI鉴别后与AP建立连接。

d) 加密功能

终端在成功完成WAI鉴别后，应使用WPI加密方式进行数据传输。

e) 密钥更新功能

终端应支持响应由AP发起的密钥更新过程，与AP协商更新会话密钥。

f) 否定非法证书功能

安装非法证书的STA应不能与合法AP通过WAI鉴别建立连接；安装合法证书的STA应不能与安装有非法证书的AP设备通过WAI鉴别建立连接。

10.3.7 同一 AS 域内 AP 间切换功能

终端应能在同一个AS域内的不同AP间进行切换，并保持通信。

10.3.8 QoS 功能

终端支持基于DSCP的服务质量，应具备4种不同优先级，并能够区分业务的优先级，确保高优先级业务的服务质量。

10.3.9 组播功能

终端支持无误地接收和发送组播业务。

10.4 安全要求

本项要求包括：

a) 应支持 WAPI 安全机制，符合 GB 15629.11—2003、GB 15629.11—2003/XG1—2006 标准，支持国家密码管理主管部门批准的用于无线局域网的算法；。

b) 支持密钥更新功能，包括单播密钥更新、组播密钥更新和基密钥更新；

c) WAPI-Cert 工作模式下，应支持 GB/T 16264.8—2005 中规定的 X.509 v3 证书，证书格式包括 PEM (X.509)、PKCS#12 (X.509)；

d) WAPI-PSK 工作模式下，应支持手工设置预共享密钥，预共享密钥应支持 ASCII 码和十六进制两种输入方式；

e) 可支持终端设备产生 WAPI 密钥对并生成证书申请文件（符合 PKCS#10 证书请求标准），证书私钥数据以受保护方式进行存储，包括加密存储或专用硬件模块等方式。

10.5 性能要求

10.5.1 吞吐量

终端在WAPI安全方式下进行数据传输时的无线接口吞吐量应满足：

- a) GB 15629.1102 (11b) 模式：下行吞吐量 ≥ 4.5 Mbit/s，上行吞吐量 ≥ 4.5 Mbit/s；
- b) GB 15629.1101 (11a) 模式：下行吞吐量 ≥ 18 Mbit/s，上行吞吐量 ≥ 18 Mbit/s；
- c) GB 15629.1104 (11g) 模式：下行吞吐量 ≥ 18 Mbit/s，上行吞吐量 ≥ 18 Mbit/s；
- d) 11n 模式：下行吞吐量 ≥ 32 Mbit/s，上行吞吐量 ≥ 32 Mbit/s；
- e) 11ac 模式：下行吞吐量 ≥ 36 Mbit/s，上行吞吐量 ≥ 36 Mbit/s；
- f) 11ax 模式：下行吞吐量 ≥ 48 Mbit/s，上行吞吐量 ≥ 48 Mbit/s。

10.5.2 时延

终端在WAPI安全方式下传输时的单向时延不大于50 ms。

10.5.3 抖动

终端在WAPI安全方式下传输时的最大抖动不大于50 ms。

10.5.4 丢包率

终端在WAPI安全方式下传输时的丢包率不大于1%。

10.5.5 接收灵敏度

终端接收灵敏度应符合YD/T 1484的规定。

10.6 运行环境要求

10.6.1 工作温度

室内型：0℃~45℃。

室外型：-15℃~55℃。

10.6.2 存储温度

室内外均为-40℃~55℃。

10.6.3 工作湿度

室内外均为10%~95% RH不凝结。

10.6.4 存储湿度

室内外均为10%~95% RH不凝结。

10.6.5 大气压

应能在以下大气压条件下的环境中正常工作：86 kPa~106 kPa。

10.6.6 电磁兼容性

本项要求包括：

- a) 终端的传导杂散骚扰应满足 YD/T 1312.2—2004 中 8.1 的限值要求；
- b) 终端的辐射杂散骚扰应满足 YD/T 1312.2—2004 中 8.2 的限值要求；
- c) 终端的连续骚扰应满足 YD/T 1312.2—2004 中 8.3、8.4、8.5、8.6 的限值要求；
- d) 终端的谐波电流应满足 YD/T 1312.2—2004 中 8.7 的限值要求；
- e) 终端的静电放电抗扰度应满足 YD/T 1312.2—2004 中 9.1 的限值要求；
- f) 终端的辐射骚扰抗扰度应满足 YD/T 1312.2—2004 中 9.2 的限值要求；
- g) 终端的电快速瞬变脉冲群抗扰度应满足 YD/T 1312.2—2004 中 9.3 的限值要求；
- h) 终端的浪涌抗扰度应满足 YD/T 1312.2—2004 中 9.4 的限值要求；
- i) 终端的射频场感应的传导骚扰抗扰度应满足 YD/T 1312.2—2004 中 9.5 的限值要求；
- j) 终端的工频磁场抗扰度应满足 YD/T 1312.2—2004 中 9.6 的限值要求。

10.6.7 运行电气条件

220 V（单相）波动范围：220 V $\pm$ 22 V，50 Hz $\pm$ 1 Hz。