

ICS 33.040

M 10



中华人民共和国通信行业标准

YD/T 2696-2014

公众无线局域网安全防护要求

Security protection requirements
for public wireless local area network

2014-10-14 发布

2014-10-14 实施

中华人民共和国工业和信息化部 发布

目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
3.1 术语和定义	1
3.2 缩略语	4
4 PWLAN 安全防护概述	5
4.1 PWLAN 安全防护范围	5
4.2 PWLAN 安全风险分析	5
4.3 PWLAN 安全防护内容	6
5 PWLAN 安全防护要求	6
5.1 第1级要求	6
5.2 第 2 级要求	9
5.3 第 3 级要求	10
5.4 第 4 级要求	11
5.5 第 5 级要求	11
附录 A (规范性附录) PWLAN 风险分析	12

前 言

本标准是“电信网和互联网安全防护体系”系列标准之一，该系列标准的结构及名称预计如下：

1. 《电信网和互联网安全防护管理指南》
2. 《电信网和互联网安全等级保护实施指南》
3. 《电信网和互联网安全风险评估实施指南》
4. 《电信网和互联网灾难备份及恢复实施指南》
5. 《固定通信网安全防护要求》
6. 《移动通信网安全防护要求》
7. 《互联网安全防护要求》
8. 《增值业务网—消息网安全防护要求》
9. 《增值业务网—智能网安全防护要求》
10. 《接入网安全防护要求》
11. 《传送网安全防护要求》
12. 《IP承载网安全防护要求》
13. 《信令网安全防护要求》
14. 《同步网安全防护要求》
15. 《支撑网安全防护要求》
16. 《非核心生产单元安全防护要求》
17. 《电信网和互联网物理环境安全等级保护要求》
18. 《电信网和互联网管理安全等级保护要求》
19. 《固定通信网安全防护检测要求》
20. 《移动通信网安全防护检测要求》
21. 《互联网安全防护检测要求》
22. 《增值业务网—消息网安全防护检测要求》
23. 《增值业务网—智能网安全防护检测要求》
24. 《接入网安全防护检测要求》
25. 《传送网安全防护检测要求》
26. 《IP承载网安全防护检测要求》
27. 《信令网安全防护检测要求》
28. 《同步网安全防护检测要求》
29. 《支撑网安全防护检测要求》
30. 《非核心生产单元安全防护检测要求》

31. 《电信网和互联网物理环境安全等级保护检测要求》
32. 《电信网和互联网管理安全等级保护检测要求》
33. 《域名系统安全防护要求》
34. 《域名系统安全防护检测要求》
35. 《网上营业厅安全防护要求》
36. 《网上营业厅安全防护检测要求》
37. 《WAP网关系统安全防护要求》
38. 《WAP网关系统安全防护检测要求》
39. 《电信网和互联网信息服务业务系统安全防护要求》
40. 《电信网和互联网信息服务业务系统安全防护检测要求》
41. 《增值业务网 即时消息业务系统安全防护要求》
42. 《增值业务网 即时消息业务系统安全防护检测要求》
43. 《域名注册系统安全防护要求》
44. 《域名注册系统安全防护检测要求》
45. 《移动互联网应用商店安全防护要求》
46. 《移动互联网应用商店安全防护检测要求》
47. 《互联网内容分发网络安全防护要求》
48. 《互联网内容分发网络安全防护检测要求》
49. 《互联网数据中心安全防护要求》
50. 《互联网数据中心安全防护检测要求》
51. 《移动互联网应用安全防护要求》
52. 《移动互联网应用安全防护检测要求》
53. 《公众无线局域网安全防护要求》(本标准)
54. 《公众无线局域网安全防护检测要求》
55. 《电信网和互联网安全防护基线配置要求及检测要求 网络设备》
56. 《电信网和互联网安全防护基线配置要求及检测要求 安全设备》
57. 《电信网和互联网安全防护基线配置要求及检测要求 操作系统》
58. 《电信网和互联网安全防护基线配置要求及检测要求 数据库》
59. 《电信网和互联网安全防护基线配置要求及检测要求 中间件》
60. 《电信网和互联网安全防护基线配置要求及检测要求 Web应用系统》
61. 《电信和互联网用户个人电子信息保护通用技术要求和管埋要求》
62. 《电信和互联网用户个人电子信息保护检测要求》

本标准与YD/T xxxx -xxxx《公众无线局域网安全防护检测要求》配套使用。

随着电信网和互联网的发展,将不断补充和完善电信网和互联网安全防护体系的相关标准。

本标准按照GB/T1.1-2009给出的规则起草。

本标准附录A为规范性附录。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：工业和信息化部电信研究院、中国联合网络通信集团有限公司、中国电信集团公司、中国移动通信集团公司、北京启明星辰信息技术股份有限公司。

本标准主要起草人：张彦超、谢 玮、龚双瑾、卜 哲、廖 璇、魏 薇、封 莎、崔 涛、杨淑敏、张佳琦、王新峰、陈 军、杨晓光、李祥军、崔 鹏。

公众无线局域网安全防护要求

1 范围

本标准规定了公众无线局域网分安全保护等级的安全防护要求，涉及到业务安全、设备及软件系统安全、网络安全、物理环境安全和管理安全。

本标准适用于基础电信业务经营者和增值电信业务经营者建设或者运营的公众无线局域网。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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。

YD/T 1731-2008 《电信网和互联网灾难备份及恢复实施指南》

YD/T 1754-2008 《电信网和互联网物理环境安全等级保护要求》

YD/T 1756-2008 《电信网和互联网管理安全等级保护要求》

YD/T 2698-2014 《电信网与互联网安全防护基线配置要求及检测要求 网络设备》

YD/T 2700-2014 《电信网与互联网安全防护基线配置要求及检测要求 数据库》

YD/T 2701-2014 《电信网与互联网安全防护基线配置要求及检测要求 操作系统》

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

无线局域网 Wireless Local Area Networks

采用无线工作方式，空中接口采用载波侦听多路访问/碰撞避免(CSMA/CA)技术实现共享媒质接入控制的一种局域网技术。无线局域网只涉及空中接口的物理层(PHY)和媒质接入控制层(MAC)，对上层协议透明。无线局域网一般工作在2.4GHz或5.8GHz频段。在本标准中，无线局域网指空中接口采用IEEE802.11标准族规定的空中接口协议。

3.1.2

公众无线局域网 Public Wireless Local Area Networks

利用无线局域网(WLAN)、IP、Web等技术组建并为公众提供网络接入服务的网络。

3.1.3

公众无线局域网安全等级 Security Classification of Public Wireless Local Area Network

公众无线局域网安全重要程度的表征。重要程度可从公众无线局域网受到破坏后，对国家安全、社会秩序、经济运行、公共利益、网络和业务运营商造成的损害来衡量。

3.1.4

公众无线局域网安全等级保护 Classified Security Protection of Public Wireless Local Area Network

对公众无线局域网分等级实施安全保护。

3.1.5

公众无线局域网安全风险 Security Risk of Public Wireless Local Area Network

人为或自然的威胁可能利用公众无线局域网中存在的脆弱性导致安全事件的发生及其对组织造成的影响。

3.1.6

公众无线局域网安全风险评估 Security Risk Assessment of Public Wireless Local Area Network

运用科学的方法和手段，系统地分析公众无线局域网所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和安全措施。防范和化解公众无线局域网安全风险，或者将风险控制在可接受的水平，为最大限度地为保障公众无线局域网的安全提供科学依据。

3.1.7

公众无线局域网资产 Asset of Public Wireless Local Area Network

公众无线局域网中具有价值的资源，是安全防护保护的对象。公众无线局域网中的资产可能是以多种形式存在，无形的、有形的、硬件、软件，包括物理布局、通信设备、物理线路、数据、软件、文档、规程、业务承载能力、人员、管理等各种类型的资源。公众无线局域网中的典型资产包括AC、AP、Radius、Web Portal等。

3.1.8

公众无线局域网威胁 Threat of Public Wireless Local Area Network

可能导致对公众无线局域网产生危害的不希望事件潜在起因，它可能是人为的，也可能是非人为的；可能是无意失误，也可能是恶意攻击。

3.1.9

公众无线局域网脆弱性 Vulnerability of Public Wireless Local Area Network

脆弱性是公众无线局域网中存在的弱点、缺陷与不足，不直接对公众无线局域网资产造成危害，但可能被公众无线局域网威胁所利用从而危及公众无线局域网资产的安全。

3.1.10

公众无线局域网灾难 Disaster of Public Wireless Local Area Network

由于各种原因，造成公众无线局域网故障或瘫痪，使公众无线局域网支持的业务功能停顿或服务水平不可接受、达到特定的时间的突发性事件。

3.1.11

公众无线局域网灾难备份 Backup for Disaster Recovery of Public Wireless Local Area Network

为了公众无线局域网灾难恢复而对相关的网络要素进行备份的过程。

3.1.12

公众无线局域网灾难恢复 Disaster Recovery of Public Wireless Local Area Network

为了将公众无线局域网从灾难造成的故障或瘫痪状态恢复到正常运行状态或部分正常运行状态、并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态，而设计的活动和流程。

3.1.13

无线破解攻击 Wireless Crack Attack

攻击者使用工具，通过捕获802.11报文，采用逆向算法获得WLAN网络密钥，或者通过弱口令字典，并辅以不断尝试认证，对WLAN网络进行暴力破解，达到入侵的目的。

3.1.14

无线钓鱼攻击 Wireless Fishing Attack

攻击者通过工具或者搭建软AP，在目标WLAN网络附近，构造与目标WLAN网络相同或者相近的网络，引诱被害者连接，一旦连接建立，攻击者会进一步截获被害者的网络流量，获取敏感信息。

3.1.15

无线中间人攻击 Wireless Man-In-The-Middle Attack

攻击者通过伪造WLAN网络标识、MAC地址等物理信息，对特定用户的无线通信进行欺骗，使得正常的通信流量流经攻击者，攻击者可以在流量中插入攻击代码或截获流量中的敏感信息，发起进一步的攻击。

3.1.16

无线DoS攻击 Wireless Denial of Service Attack

攻击者通过向WLAN网络中发送大量伪造的认证、关联等802.11报文，从而达到让AP或AC过载的目的，使得正常用户无法接入WLAN网络；或者通过发送大量伪造的去认证、去关联等802.11报文，拆除已经建立的WLAN连接，导致用户无法通过WLAN网络接入。

3.1.17

无线注入攻击 Wireless Injection Attack

攻击者通过伪造802.11报文，向WLAN网络中注入流量，例如通过注入ARP Request（地址解析协议请求），对WLAN进行干扰，达到加快破解的目的；通过无线注入攻击，攻击者也可以伪造网络向量分配，抢占WLAN信道通信时间，实现拒绝服务攻击；攻击者也可以通过注入更为复杂的流量，达到网络欺骗的目的。

3.1.18

HotSpotter攻击 Hotspotter Attack

攻击者监测WLAN网络中的探测请求，并将发现的WLAN网络与自身的WLAN热点列表进行对比，如果一旦发现匹配的WLAN网络，攻击发起者会伪造认证和关联过程，引诱用户，一旦连接建立，攻击者会进一步对受害者进行毒化或扫描，并发起进一步的攻击。

3.1.19

SQL注入攻击 Sql Injection

SQL注入是一个代码注入技术，它利用一个Web应用程序的安全漏洞，在数据库层实施攻击。如果对用户输入的非合法字符串（如Web表单递交或输入域名或页面请求的查询字符串）过滤不严谨，则会把构建的恶意SQL语句传递到数据库，欺骗服务器执行恶意的SQL命令中执行。

3.1.20

跨站脚本攻击 Cross Site Scripting

一种Web应用程序的漏洞类型，能令攻击者插入客户端脚本到Web页面，当其他用户查看时被攻击。

3.1.21

网页木马 Web-Page Trojan

表面上伪装成普通的网页文件或是将恶意的代码直接插入到正常的网页文件中，当有人访问时，网页木马就会利用对方系统或者浏览器的漏洞自动将配置好的木马的服务端下载到访问者的电脑上来自动执行。

3.1.22

TCP拒绝服务 TCP Flood

一种拒绝服务攻击，利用TCP协议缺陷，发送大量伪造的TCP连接请求，从而使得被攻击方资源耗尽（CPU满负荷或内存不足）的攻击方式。

3.1.23

Portal 服务器 Portal Server

Portal是一种Web应用，通常用来提供个性化、单点登录、聚集各个信息源的内容，并作为信息系统表现层的宿主。聚集是指将来自各个信息源的内容集成到一个Web页面里的活动。

3.2 缩略语

下列缩略语适用于本标准。

AC	Access Point Controller	接入控制器
ACL	Access Control List	访问控制列表
AP	Access Point	接入点
BGP	Border Gateway Protocol	边界网关协议
BRAS	Broadband Remote Access Server	宽带接入服务器
DDoS	Distributed Denial of Service	分布式拒绝服务攻击
DNS	Domain Name System	域名系统
DSL	Digital Subscriber Line	数字用户专线
HA	High Availability	高可用性
HTTP	Hypertext Transfer Protocol	超文本传输协议
IP	Internet Protocol	网际协议
ISIS	Intermediate system to intermediate system	中间系统到中间系统
MAC	Media Access Control	介质访问控制
OSPF	Open Shortest Path First	开放式最短路径优先
PON	Passive Optical Network	无源光纤网络
PWLAN	Public Wireless Local Area Network	公众无线局域网
RADIUS	Remote Authentication Dial In User Service	远程访问拨号接入用户服务
SQL	Structured Query Language	结构化查询语言
SSH	Secure Shell	安全外壳协议
WIPS	Wireless Intrusion Prevention System	无线入侵防御系统
WLAN	Wireless Local Area Networks	无线局域网
XSS	Cross Site Script	跨站脚本攻击

4 PWLAN 安全防护概述

4.1 PWLAN 安全防护范围

公众无线局域网（PWLAN）是指利用无线局域网（WLAN）、IP、Web等技术组建并为公众提供网络接入服务的网络。

PWLAN网络结构有三种，分别为传统自治型胖AP、新型集中管理型瘦AP-AC直挂方式、新型集中管理型瘦AP-AC旁挂方式，如图1所示。PWLAN主要设备包括AC、AP、热点交换机、BRAS、关口（Portal）服务器、采用Radius等协议的认证服务器等；其主要功能是对使用PWLAN的用户进行认证、授权和计费，并利用接入技术实现无线接入。

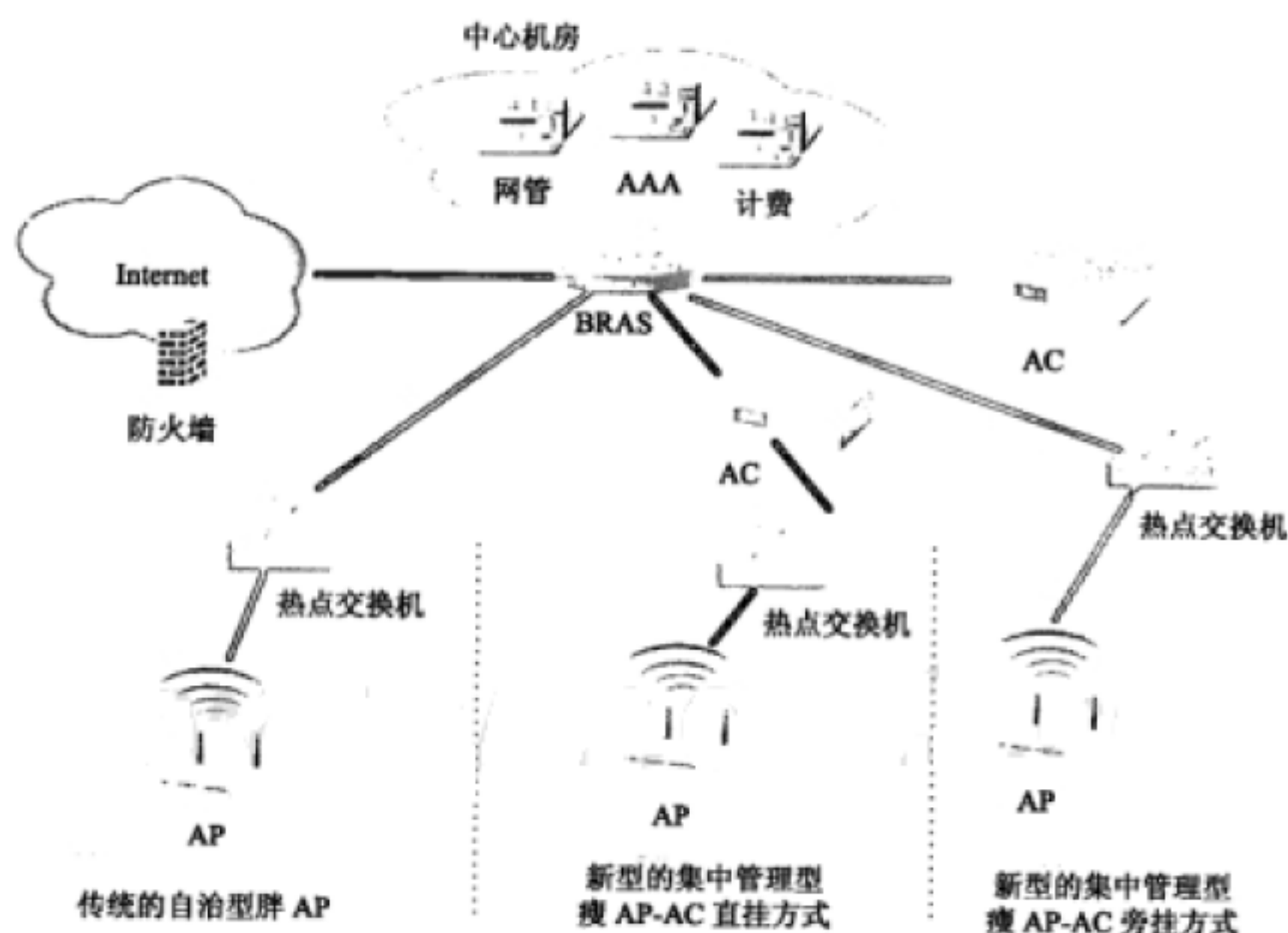


图1 PWLAN 网络结构示意图

PWLAN安全防护范畴主要包括上述PWLAN中的软硬件以及产生和处理的数据等。

本标准主要针对PWLAN提出安全防护要求，与PWLAN相关的其他网络单元如接入网、IP承载网、支撑网等的安全防护要求见相应网络类型的安全防护标准。

4.2 PWLAN 安全风险分析

PWLAN中的重要资产至少应包括：

- ◆ PWLAN 设备：AC、AP、BRAS、Radius、Web Portal 等。
- ◆ PWLAN 数据：AC 标识、AP 标识、设备配置信息、认证信息、话单信息等。
- ◆ PWLAN 其他的资产（如文档、人员等）可见附录 A 表 A.1 对资产的分类及举例。

PWLAN 在设备部署、配置、系统管理等环节上均可能引入安全脆弱点，如各类 AC、AP 等设备在软硬件安全方面存在的漏洞以及无线网络架构可能存在安全域未划分、无冗余备份等脆弱性。PWLAN 的脆弱性分析应包括但不限于附录 A 表 A.2 所列范围。

PWLAN 的威胁根据来源可分为技术威胁、环境威胁和人为威胁。环境威胁包括自然界不可抗的威胁和其他物理威胁。根据威胁的动机，人为威胁又可分为恶意和非恶意两种。PWLAN 的威胁分析应包括但不限于附录 A 表 A.3 所列范围。

PWLAN 可能存在的安全脆弱性被利用后会产生很大的安全风险，突出的安全风险如：

- 1) PWLAN 向用户推送的认证页面（Web Portal）信息被篡改；
- 2) 用户认证等隐私信息被窃取；
- 3) 逃避计费；
- 4) 计费数据被篡改或替换；
- 5) 网络被攻击后不可用等。

4.3 PWLAN 安全防护内容

PWLAN安全防护内容及要求可划分为业务安全、设备及软件系统安全、网络安全、物理环境安全、管理安全等五个层面。其中：

——业务安全

主要包括业务认证管理、业务资源控制、业务安全防范、业务安全审计等方面的安全要求。

——设备及软件系统安全

主要包括PWLAN相关网络设备、通用主机设备、操作系统和数据库等方面安全要求。

——网络安全

主要包括PWLAN相关系统层面的结构拓扑、网络保护与恢复、网络管理和网络攻击防范等方面的安全要求。

——物理环境安全

主要包括机房位置、电力供应、防火、防水、防静电、温湿度控制等方面的安全要求。

——管理安全

主要包括机构、人员、制度、日常运维、安全监控、风险评估、应急预案等方面的安全要求。

5 PWLAN 安全防护要求

5.1 第 1 级要求

5.1.1 业务安全要求

5.1.1.1 业务认证管理

- a) 应对登录用户进行身份标识和鉴别。
- b) 应采用加密方式传输用户的口令信息。
- c) 应采用加密方式存储用户的口令信息。

5.1.1.2 业务资源控制

用户异常掉线后，AC、AP应释放内存，回收资源，防止黑客发起的拒绝服务攻击。

5.1.1.3 业务安全防范

a) 应具备发现和处理含有恶意代码链接的能力，防止用户访问PWLAN登录页面被非法利用窃取用户信息。

b) 应具备防护SQL注入攻击和变种注入攻击的能力，保护Portal页面和PWLAN设备Web管理界面，防止PWLAN数据库中的敏感数据被非授权读取、篡改。

c) 应具备URL访问控制能力，避免恶意用户利用PWLAN系统内相关web页面业务逻辑漏洞实施威胁性攻击或绕过认证计费非授权访问公众互联网。

5.1.1.4 业务安全审计

a) 审计范围应覆盖到每个用户的关键操作、重要行为、业务资源使用情况等重要事件，如普通用户异常登录、发布恶意代码、异常修改账号信息等行为以及管理员在业务功能和账号控制方面的关键操作等。

b) 应保护审计记录，保证无法删除、修改或覆盖等。

c) 业务相关审计记录应包括事件日期、时间、发起者信息、类型、描述和结果等。

5.1.2 设备及软件系统安全要求

5.1.2.1 AC、AP 及热点交换机设备

a) AC设备在应用层应对Cookies或者Session做判断，防止任意用户在不通过验证的情况下下载设备配置文件，进而破解管理员密码，获得AC的控制权。

b) AC、Radius设备应支持SSH、HTTPS等加密形式登陆。

c) AC设备应开启防护功能，包括端口隔离、用户隔离、非法AP检测等功能。

d) AP设备和热点交换机应开启二层隔离功能。

e) AC设备上应配置ACL，防止DNS隧道（DNS Tunnel）攻击绕过认证机制。

5.1.2.2 网络设备

PWLAN相关网络设备主要包括各类交换机设备等，相关网络设备应满足YD/T 2700-2014《电信网与互联网安全防护基线配置要求及检测要求 网络设备》的安全要求。

5.1.2.3 数据库

数据库的安全应满足YD/T 2700-2014《电信网与互联网安全防护基线配置要求及检测要求 数据库》的安全要求。

5.1.2.4 操作系统

操作系统的安全应满足YD/T 2700-2014《电信网与互联网安全防护基线配置要求及检测要求 操作系统》的安全要求。

5.1.3 网络安全要求

5.1.3.1 网络拓扑

PWLAN节点部署合理，具有较高的可用性和可扩展性。

5.1.3.2 网络保护与恢复

a) PWLAN节点重要部件和模块（如电源模块、主控模块等）应配置为主备用方式。

b) PWLAN重要节点（如AC、BRAS等）间链路应采取链路冗余保护措施，以保证网络具有抗灾以及灾难恢复能力。

c) PWLAN应根据应用的需求采用链路聚合、保护倒换等安全保护措施。

5.1.3.3 网络管理

a) PWLAN应根据网络结构形式采用分域的管理方式，并根据实际需求或运维体制设置分级权限，实现对网络的灵活管理。

b) PWLAN业务网络与运维、管理、监测等辅助系统（或平台）间应实现逻辑隔离，并启用安全域访问控制策略，严格限制对有关设备的访问。

c) PWLAN网络管理应使用用户安全鉴别和认证措施。

d) PWLAN应有与当前网络节点、链路、频谱等资源配置和运营情况相符合的网络拓扑图（或记录完整拓扑信息的运维文档）。

e) PWLAN的网络管理应启用访问和资源控制的安全措施，遵循最小特权原则对接口使用、访问和资源等进行限制。

f) PWLAN管理信息及数据的机密性和完整性在传送、接收、处理和存储过程中都应得到保证。

5.1.3.4 网络安全监测

a) 应具备关键设备（AC、Radius）和数据库运行状态监测功能，集中监控和展现PWLAN设备网络运行状态、CPU和内存等运行状态信息以及在线用户数量、信道使用情况等信息，同时需要实现数据库的版本信息、表空间利用率和数据库表操作记录等运行监测。

b) 应具备安全告警事件监测功能，应实现对PWLAN网络设备和各种安全设备以及接入认证系统产生的安全告警日志的分析和监测功能，实现安全事件告警的及时监测和有效处理。

5.1.3.5 网络安全防范

a) PWLAN应具有防范常见网络攻击、差错防范和处理的能力，在无线接入边界部署和启用攻击、入侵防范技术手段，防范针对AC、热点交换机等网络设备和Radius、Portal服务器等IT系统的常见攻击及入侵。

b) 应防止远程入侵计费系统。

c) PWLAN应具有防范通过空口进行的网络入侵行为的能力，避免通过逆向、暴力破解等方式入侵到PWLAN内网，导致PWLAN数据安全受到威胁。

d) PWLAN应具有防范通过空口进行的网络欺骗行为的能力，避免非法AP接入AC、无线钓鱼等风险，防止用户登录PWLAN的账号密码以及网厅、邮箱等互联网应用账号信息被非法窃取。

e) PWLAN应具备防范常见的应用层攻击的能力，如Http-Flood（Http协议的DDoS攻击）等。

f) PWLAN相关设备、系统对各类管理和维护用户应启用登录失败保护和处理措施。

g) 网络设备的软件应具备实时操作、信息处理、更新升级、差错防护、故障定位等功能。

h) PWLAN建立具有介质存取、验证和转储制度，确保备份数据授权访问。

i) 应至少区分并设置PWLAN的网络管理域、设备管理域、用户接入域等不同功能区域，利用VLAN、IP、防火墙等技术措施隔离，防止跨域访问，并在域边界处实施严格的双向访问控制，防止域用户非授权访问网络资源，尤其做好公共互联网与管理域、管理域与用户接入域之间的隔离。

5.1.4 物理环境安全要求

a) 应满足YD/T 1754-2008《电信网和互联网物理环境安全等级保护要求》中第1级的相关要求。

b) AP设备应防止盗用、替换，室外AP设备应具备防雨、雪、风砂、雷击等防护措施。

5.1.5 管理安全要求

a) 应满足YD/T 1756-2008《电信网和互联网管理安全等级保护要求》中第1级的相关要求。

b) PWLAN安全风险评估至少应覆盖业务安全、设备及软件系统安全、网络安全、物理环境安全等相关技术风险和人员安全、运维安全等相关管理风险，至少包含PWLAN相关资产、脆弱性、威胁、安全措施、风险分析等要素和内容，并根据评估结果制定相应的风险处理计划。

c) PWLAN应按照YD/T1731-2008《电信网和互联网灾难备份及恢复实施指南》的相关要求制定灾难恢复预案，并定期组织灾难恢复预案的教育培训和演练。

5.2 第2级要求

5.2.1 业务安全要求

5.2.1.1 业务认证管理

除满足第1级的要求之外，还应满足：

a) 应能防止身份鉴别暴力攻击（如登录模块应采用随机验证码进行验证，并且保证验证码不易被自动预测、识别）。

b) 应具有防范利用AP或用户认证报文发起攻击的能力，如泛洪攻击、中间人攻击、欺骗等。

5.2.1.2 业务资源控制

除满足第1级的要求之外，还应满足：

具有防止过度访问、拒绝服务攻击等的保护机制。

5.2.1.3 业务安全防范

除满足第1级的要求之外，还应满足：

a) 应具备防护无线中间人攻击的能力，防止伪造MAC地址在AP和用户之间进行欺骗攻击。

b) POATATL页面应具备防攻击、防篡改的能力。

5.2.1.4 安全审计

除满足第1级的要求之外，还应满足：

应具备对审计记录数据进行统计、查询、分析及生成审计报表的功能。

5.2.2 设备及软件系统安全要求

5.2.2.1 AC、AP及热点交换机设备

除满足第1级的要求之外，还应满足：

使用安全漏洞扫描设备定期对所有PWLAN相关设备（AC、Radius、Web Portal等）进行安全漏洞扫描，检查有无高中风险安全漏洞，并及时对漏洞进行修补。

5.2.2.2 网络设备

同第1级要求。

5.2.2.3 数据库

同第1级要求。

5.2.2.4 操作系统

同第1级要求。

5.2.3 网络安全要求

5.2.3.1 网络拓扑

同第1级要求。

5.2.3.2 网络保护与恢复

除满足第1级的要求之外，还应满足：

a) PWLAN相关关键数据（如业务数据、配置数据、性能数据、告警数据等）应有本地数据备份，并按介质特性对备份数据进行定期的有效性验证。

b) PWLAN网络灾难备份和恢复时间应满足行业管理、网络和业务运营商应急预案的要求。

5.2.3.3 网络管理

除满足第1级的要求之外，还应满足：

PWLAN网络管理原则上应具有对业务相关数据进行检测、统计、控制、过滤的功能。

5.2.3.4 网络安全监测

除满足第1级的要求之外，还应满足：

a) 应具备空口无线安全事件监测功能，监测PWLAN网络中的以下安全事件：WLAN DoS攻击（去认证泛洪、去关联泛洪、客户端过载等）、WLAN HotSpotter攻击、WLAN中间人攻击、WLAN干扰和WLAN报文注入攻击等。

b) 应具备AP配置实时监测功能，对AP的各种安全漏洞和配置弱点信息进行监测和展现。

5.2.3.5 网络安全防范

除满足第1级的要求之外，还应满足：

a) 应防止非授权使用网络，如利用DNS隧道（DNS Tunnel）绕过认证机制上网。

b) 应防止利用PWLAN中网络地址划分安全域隔离缺陷，导致直接入侵控制。

c) 应具有防范通过空口进行的无线拒绝服务攻击的能力，避免认证/去认证泛洪攻击、抢占射频时间片攻击、射频干扰等风险，防止由于PWLAN工作异常而导致不能提供服务。

d) 与PWLAN及其业务相关联的运维、管理、监测等系统的应用应当限制和禁用可能造成漏洞的服务和端口，应在系统边界启用必要的防攻击、防入侵措施（如安装和使用防火墙、入侵检测、无线入侵防御等安全设备等），系统相关软件应及时安装补丁，定期检查更新，及时消除可能的隐患。

e) PWLAN和相关系统内部署的安全设备在发生攻击或入侵时，应能及时准确的提供攻击或入侵的告警、监测信息

f) PWLAN各类设备及系统应启用完整的安全日志功能，并实现日志的管理和安全审计，日志记录保存时间不少于90天、审计记录保存时间不少于180天。日志应包含访问、配置、状态、统计、告警等安全相关事件的来源、时间、描述等信息内容。

g) 不应出现Owasp Top10所列的高危Web安全漏洞。

5.2.4 物理环境安全要求

除满足第1级的要求之外，还应满足：

应满足YD/T 1754-2008《电信网和互联网物理环境安全等级保护要求》中第2级的相关要求。

5.2.5 管理安全要求

除满足第1级的要求之外，还应满足：

a) 应满足YD/T 1756-2008《电信网和互联网管理安全等级保护要求》中第2级的相关要求；

b) 应定期对PWLAN各类设备、系统进行安全风险评估（每两年至少评估一次，重大活动、节日前应进行评估）。

c) PWLAN应设有专职的操作、维护技术人员和安全管理人員，应定期组织对相关人员进行技术培训和考核。

d) 应定期组织PWLAN各类设备、系统灾难恢复预案的教育培训和演练。

e) 应定期对PWLAN空口信号进行安全风险评估。

5.3 第3级要求

5.3.1 业务安全要求

同第2级要求。

5.3.2 设备及软件系统安全要求

同第2级要求。

5.3.3 网络安全要求

同第2级要求。

5.3.4 物理环境安全要求

同第2级要求。

5.3.5 管理安全要求

除满足第2级的要求之外，还应满足：

应定期对PWLAN各类设备、系统进行安全风险评估（每年至少评估一次，重大活动、节日前应进行评估）。

5.4 第4级要求

安全等级为第4级的PWLAN的安全要求待补充。

5.5 第5级要求

安全等级为第5级的PWLAN的安全要求待补充。

附 录 A
(规范性附录)
PWLAN 风险分析

本附录介绍了 PWLAN 风险分析过程中可用于资产、脆弱性、威胁识别和分析的分类方法。

A.1 资产分析

PWLAN资产的识别与选取应符合科学性、合理性。PWLAN资产大致包括各类设备/主机、数据信息、文件、人员、物理环境设施等。PWLAN的资产分析应包括但不限于表A.1所列范围。

表 A.1 资产类别

类别	资产
网络设备/主机	数据网络设备（如各类 AC、AP、交换机等）； 通用主机设备（如各类服务器、工作站、终端、数据库等）； 其他设备（如各类安全设备、辅助设备 etc）； 线路等。 (网络设备/主机资产中可包含与设备/主机直接相关且没有必要细分的软、硬件及相关附件)
独立软件	有必要独立识别的软件（如应用软件、系统程序、数据库等）
文档/数据	数据信息（如网络、设备、功能系统相关的各类业务、配置、管理等方面的数据和信息等）； 文档资料（如各类形式设计文档、技术手册、管理规定、工作计划、财务报告、数据记录等）
服务/业务	网络、各功能/业务系统提供的各类服务和业务等
网络资源	与网络相关的链路、带宽、各类设备容量、网络地址空间等资源
人员	各类人员以及相关技术经验、组织、管理机制（如掌握相关技术的网络维护人员和设备维护人员、安全管理组织和机构、安全管理机制等）
环境/设施	机房和各类设备设施（如电力供应系统、电磁防护系统、防火和防潮系统、防静电系统、防雷击系统、温湿度控制系统等）

A.2 脆弱性分析

PWLAN的脆弱性包括技术脆弱性和管理脆弱性两个方面。脆弱性识别对象应以资产为核心。PWLAN的脆弱性分析应包括但不限于表A.2所列范围。

表 A.2 脆弱性类别

类别	对象	脆弱性
技术脆弱性	网络	网络规划和拓扑、设备部署、资源配置的缺陷等； 网络保护和恢复能力的缺陷、安全技术措施和策略等方面的漏洞等； 业务相关的接入、访问、服务优先级、资源管理、数据信息检查和过滤等业务接入管理方面的缺陷和漏洞等
	设备/主机	各类 AC、AP、路由器、交换机等设备在软硬件安全方面存在的漏洞等； 可靠性、稳定性、业务支持能力和数据处理能力、容错和恢复能力的缺陷等； 设备访问的连接、授权、鉴别、代理和控制等方面的安全漏洞，以及授权接入的口令、方式、安全连接、用户鉴别、代理等访问控制方面存在的漏洞隐患等； 相关数据信息在使用、传送、备份、保存、恢复等环节的安全保护技术缺陷和安全策略的漏洞等

表 A.2 (续)

类别	对象	脆弱性
技术脆弱性	数据	数据泄露、非授权访问
	物理环境	包括物理环境安全防护能力的缺陷等(如可分为机房场地选择、防火、供配电、防静电、接地与防雷、电磁防护、温湿度控制、通信线路、机房设施及设备的安全防护能力缺陷等)
管理脆弱性		<p>包括网络相关的方案和预案、人员、保障、组织等安全机制和管理制度在制定和实施等环节的漏洞和缺陷等。</p> <p>可分为安全管理机构、安全管理制度、人员安全管理、建设管理、运维管理等方面。其中，安全管理机构方面(如岗位设置、授权和审批程序、沟通和合作等)；</p> <p>安全管理制度方面(如管理制度及相应的评审和修订等)；</p> <p>人员安全管理方面(如人员录用、上岗、安全培训、组织、访问控制等)；</p> <p>建设管理方面(如安全方案不完善、软件开发不符合程序、工程实施未进行安全验收或验收不严格等)；</p> <p>运维管理方面(如物理环境管理、设备维护、技术支持、关键性能指标监控、攻击防范措施、数据备份和恢复、访问控制、操作管理、应急保障措施等)</p>

A.3 威胁分析

PWLAN的威胁根据来源可分为技术威胁、环境威胁和人为威胁。环境威胁包括自然界不可抗的威胁和其他物理威胁。根据威胁的动机，人为威胁又可分为恶意和非恶意两种。PWLAN的威胁分析应包括但不限于表A.3所列范围。

表 A.3 威胁类别

类别	威胁
技术威胁	<p>未充分考虑冗余、可靠性及业务安全、应用需求等原因，妨碍相关功能完全实现的缺陷或隐患造成的安全事件等；</p> <p>系统差错、节点/链路可靠性等原因造成的故障等；</p> <p>错误响应和恢复等；</p> <p>相关数据、信息在备份、保存、恢复过程中发生的差错、损坏、丢失等；</p> <p>地址、带宽、处理能力、存储空间等资源的滥用、浪费和过度消耗等；</p> <p>突发流量和异常数据流量等；</p> <p>恶意代码、病毒等；</p> <p>无线网络架构自身存在的脆弱性风险，包括不安全的配置、无线钓鱼、无线中间人攻击、无线DoS攻击、射频干扰、无线破解、无线注入等风险</p>
环境威胁	物理环境
	<p>供电故障，灰尘、潮湿、温度超标，静电、电磁干扰等；</p> <p>意外事故或通信线路方面的故障等</p>
人为威胁	灾害
	<p>鼠蚁虫害；</p> <p>洪灾、火灾、泥石流、山体滑坡、地震、台风、雷电等自然灾害；</p> <p>战争、社会动乱、恐怖活动等</p>
人为威胁	人为恶意行为
	<p>针对网络的恶意拥塞，针对业务、设备等相关数据的拦截、篡改、删除等攻击行为；</p> <p>针对网络、业务数据、服务、设备进行的恶意扫描、监听、截获等嗅探行为；</p> <p>非授权访问、越权操作等；</p> <p>伪造和欺骗等；</p> <p>人为物理攻击，损坏、盗窃等</p>

表 A.3 (续)

类别		威胁
人为威胁	人为非恶意行为	误操作; 无作为、技能不足等; 相关数据、信息无意泄漏, 数据损坏和丢失等; 组织、安全管理制度不完善、制度推行不力、缺乏资源等非规范安全管理等

中华人民共和国
通信行业标准
公众无线局域网安全防护要求
YD/T 2696-2014

*

人民邮电出版社出版发行
北京市丰台区成寿寺路1号邮电出版大厦
邮政编码: 100164
北京康利胶印厂印刷
版权所有 不得翻印

*

开本: 880 × 1230 1/16 2015年9月第1版
印张: 1.5 2015年9月北京第1次印刷
字数: 36千字

15115 · 482

定价: 20元

本书如有印装质量问题, 请与本社联系 电话: (010)81055492