OSEAS 认证管理系统

白皮书

上海光辰信息技术有限公司

2016-12

目录

第1章. OSEAS 认证管理系统简介

1.1 系统简介

OSEAS RA- 2K/10K 认证管理系统为 3A 认证服务器（Authentication、Authorization、Accounting），遵循 radius 协议，提供认证、授权、计帐服务，在此基础上，针对中国移动、中国联通、中国电信 2G/3G/4G 无线 VPDN/APN 接入进行了专门的优化和功能扩充；作为企业级的安全认证产品，适用于政府、金融、交通运输、公共事业、连锁业、能源、物流等行业。

1.2 认证管理系统的特点

- ★ 专为企业级的 2G/3G/4G 无线接入应用研发，实现高安全性的企业 VPDN/APN 接入所需的安全认证功能。
- ★ 支持两台认证服务器双机实时同步，实时切换，提高系统的可靠性并提高客户端并发认证的负载能力。
- ★ 产品具备良好的处理性能和可伸缩性。
- ★ 采用数据库系统存放用户账户信息及其角色和权限定义，支持大数据流量，历史数据自动转存，支持分布式部署。
- ★ 认证系统采用 Web 方式进行管理，界面友好、操作简单、配置灵活。
- ★ 认证系统具备完善的日志和操作审计功能，便于查询、统计。

1.3 产品功能列表

OSEAS RA-2K/10K 系列接入认证系统具备以下的主要功能：

1.3.1 认证、授权、计费

- ★ 支持 CDMA、EVDO 制式的 VPDN 模式和 WCDMA、LTE 制式 的 APN 模式下的无线接入 PPP 拨号认证。
- ★ 支持多个运营商的 PPP 用户在一台（组）设备上同时进行认证。
- ★ 支持 PPP 客户端使用 PAP 和 CHAP 协议。
- ★ 支持一个域内有多个 LNS 的环境，为经由不同 LNS 发起认证请求的拨号用户对应分配不同（或相同）的 IP 地址，以满足 APN/VPDN 双线路冗余或负载平衡模式的需要。
- ★ 支持多域、多对端设备分布式结构部署，支持统一管理。
- ★ 支持按域划分多个用户组并分别授权，支持多级别权限分配和管理。
- ★ 支持为用户静态绑定 IP 地址和通过地址池（IP POOL）动态分配 IP 地址；管理员可建立多个地址池，供拨号用户以域和组为集合单独或共享方式使用。
- ★ 用户每月允许在线的总时长管理。
- ★ 用户账户的有效期管理。
- ★ 记录用户登陆、退出时间，统计在线时长和登陆次数。

1.3.2 用户管理

- ★ 用户分组及组管理员设置。
- ★ 用户账户管理：新建、修改、删除、查询。
- ★ 用户账户批量管理：批量新建、修改。
- ★ 用户账户设置：用户名、密码、所属组，用户描述。
- ★ 用户账户停用、删除。
- ★ 用户对应 IMSI 号和分配指定 IP 地址管理。
- ★ 用户 PPP 认证失败次数超限自动锁定账户。

1.3.3 安全管理

- ★ 非法登陆尝试告警：记录非法或失败登陆请求的信息并通过 MAIL，Web 页面即时提示且必须由管理员进行处理。
- ★ 密码安全管理：密码长度、复杂度、密码有效期等条件的强制约束管理。
- ★ 账户有效性和有效期管理。
- ★ 各级管理员登陆有效性管理。
- ★ 各级管理员操作记录。
- ★ 用户分级授权。

1.3.4 设备管理、维护及工具

- ★ 设置管理地址，管理方式：HTTP、HTTPS、Console/SHH Command Line。
- ★ 设置认证服务地址、端口。
- ★ 设置认证域。
- ★ 设置认证对端设备地址，认证连接口令。
- ★ 设置 IP 地址池。
- ★ 设置对端设备 IP 地址池绑定。
- ★ 设置系统时间和 NTP。
- ★ 设置备机 IP 地址，设置同步参数。

- ★ 设置 DNS 服务器地址。
- ★ 设备初始化，设备重启，设备配置导出和导入。
- ★ 网络测试工具：PING，TRACE。
- ★ 设备状态：CPU、内存占用率，在线用户数等。
- ★ 邮件提醒和报表：系统运行状态异常、认证、登陆错误邮件提醒。

1.3.5 日志

- ★ 内置日志系统记录相关日志信息。
- ★ 系统日志：记录认证服务器系统运行状况。
- ★ 用户登陆日志：账号及对应 IMSI，登陆时间，在线时长,登陆错误日志记录账号及对应 IMSI 号。
- ★ 管理员登陆日志：登陆账户，IP 地址。
- ★ 管理员操作日志。

1.3.6 统计分析查询

- ★ 在线用户统计。
- ★ 用户登陆状况统计。
- ★ 各种自定义的组合条件的分析统计查询。

1.3.7 历史数据管理

- ★ 各种自定义的组合条件的历史数据分析统计查询。
- ★ 历史数据导出转储。

1.3.8 告警功能

- ★ 系统实时状态显示。
- ★ 实时页面登陆告警。
- ★ 实时页面服务器状态告警。

★ 实时页面当前系统服务告警。

★ 即时邮件提醒：

- 用户 WEB 登陆和拨号错误即时提醒。
- 系统运行状态超出阈值即时提醒。
- 系统服务状态异常告警。

★ 周期报表邮件告警--可按日、周、月自定义邮件发送周期：

- 用户 WEB 登陆和拨号认证统计报表。
- 系统服务状态报表。
- 系统运行状态报表。

第2章. OSEAS 产品功能说明

2.1 系统设置

在系统设置功能模块中，系统管理员可以完成对认证系统、设备的参数配置、管理、维护的所需的各项功能：

2.1.1 管理设置

管理设置模块中包含了以下的功能：

★ **管理员密码设置** － 修改系统管理员密码。

★ **系统安全设置** － 设置各级用户密码强度约束，用户密码必须符合约束规则，相应的新增、修改用户密码的操作才能够生效执行。

★ **串口密码修改** － 当 OSEAS 认证系统 Console 接口密码遗忘后，通过此菜单设置 Console 接口管理员的密码。

2.1.2 基本设置

基本设置模块中包含了以下的功能：

- ★ **授权码** － 查看、升级当前系统授权码。
- ★ **IP 地址** － 配置认证服务器各网络接口的 IP 地址。
- ★ **路由设置** － 配置系统路由表，在该界面可以查看当前系统路由表记录，添加新的路由记录，修改现存的路由表记录，以及删除一条或多条记录。
- ★ **DNS 设置** － 设置 DNS 服务器，在此界面增加、修改、删除 DNS 服务器的记录，用于解析主机名、域名所对应的 IP 地址。具体地址请咨询网络提供商。
- ★ **系统时间**－设置 NTP 服务器，在此界面选择是否使用 NTP 服务器，以及设置 NTP 服务器参数，以使认证服务器的系统时间保持正确。
- ★ **备份机设置**－配置认证服务器主、备机属性，以及参数，启动实时备份。

2.2 系统工具

系统工具功能模块中，认证服务器系统提供了一系列的工具，管理员可以完成系统配置、调试、备份、恢复等相关的功能。

★ **初始化** － 初始化设备，清除所有用户配置数据，将认证服务器恢复至出厂状态。初始化后请连设备的 MGT 口，用 http://10.10.10.10:8080/oseas 登录管理页面。

★ **系统重启** － 重启认证服务器系统。

★ **系统升级** － 为 OSEAS 系统提供升级功能。

★ **监控-告警设置** － 设置当前系统的告警值，以邮件的方式进行系统告警和报表发送。

★ **PING** － 使用 PING 功能测试网络连接是否正常。

★ **跟踪路由** － 使用该功能测试到达目标地址的网络路由是否可达。

★ **备份系统配置** － 将认证服务器系统的所有的配置数据备份到管理员计算机本地磁盘保存。

★ **恢复系统配置** － 将此前所备份的系统配置恢复到认证服务器，使认证服务器系统状态、数据恢复至备份的时间点。恢复的过程中不要进行其他操作，直到系统提示恢复成功并重启服务器使配置生效。

★ **手工同步** － 手工执行同步操作，并允许系统管理员有选择的向备份机同步数据，以满足管理员即时同步变化的数据内容。

2.3 系统状态

在系统状态功能模块中，管理员可以查看认证服务器系统的相关参数，监控系统服务允许状态，监控设备的运行状态：

★ **基本状态** － 查看认证服务器的基本状态，在该页面可以查看当前的系统版本，当前的授权用户数，当前已激活的用户数，当前的处理器使用、内存使用、存储空间使用、接口地址配置等状态数据。

★ **服务状态** － 查看、启停认证服务器的认证服务、数据库、WEB、邮件和日志等服务的运行状态。

★ **统计报表**－系统会自动统计处理器、内存、磁盘使用、磁盘读写和活动网络的使用情况，用户可以具体查看每天、每周、每月、每年的详细信息。

2.4 认证服务器设置

在认证服务器设置功能模块中，系统管理员可以根据运营商所分配的参数，结合企业网络情况，对认证服务器的相关的功能参数进行配置：

★ **认证服务器配置** － 配置认证服务所绑定的网络接口，以及和对端设备通信所使用的网络端口，可以配置 1-4 个网络端口。

★ **域设置** － 配置认证域及域所绑定的地址池，具体域的数据需要结合运营商分配给用户的的数据进行配置。

★ **对端设备配置** － 配置对端设备 IP 地址和认证密钥等参数，可以配置一个或多个对端设备。

★ **IP P**ool － IP POOL 在系统中独立存在，IP POOL 可以绑定到组、域，也可以绑定到设备；管理员可以根据需要灵活的选择按组为最小的集合使用 IP POOL 动态分配 IP 地址，或者让整个域的用户或整个设备使用一个 IP POOL 动态分配 IP 地址。IP POOL 可由系统管理员和域管理员创建并配置，创建该 IP POOL 的用户被系统定义为该 IP POOL 的“拥有者”。IP POOL 有共享，不共享两种属性；共享 IP POOL 可以和地址池的创建者（系统管理员或域管理员）具备管理权限的多个组和域同时绑定；非共享 IP POOL 只能和一个组或域进行绑定。OSEAS 认证系统在为拨号用户分配地址的次序为：首先判断该用户是否是静态地址，之后根据用户所属组绑定的地址池进行动态分配，再之后根据用户所属域绑定地址池进行动态分配，最后根据设备地址池进行动态分配。

★ **设备-地址池绑定** －对端设备在使用时，需要绑定经过该设备的域、组涉及的所有 IP POOL ，或设备直接绑定地址池，认证过程根据该绑定关系进行地址分配，没有绑定关系则无法分配 IP 地址。

2.5 用户管理

在用户管理功能模块中，管理员可以完成添加、修改、删除用户组，添加、修改、删除用户账户，修改用户登陆密码等功能：

★ **组管理** － 创建、配置、管理、删除域管理员组和用户组。组绑定所属域，用户认证身份协商类型，用户失败登录次数，用户自动解锁时间，每月在线时长等信息。

★ **账户管理** － 创建、配置、管理、删除管理员、认证用户的账户，用户分组管理员、普通用户，组管理员的功能为管理域下用户组普通用户，可增删改组下的普通用户，组管理员设置必须填写用户名、用户姓名、密码，且用户名不可同其他用户重名，普通用户设置必须填写用户名，用户姓名，密码，IMSI 号码，接入号。

★ **密码管理** － 各级管理员修改下级用户密码，及用户自助方式修改密码。

★ **修改密码** － 当前登陆用户修改密码。

2.6 统计查询

在统计查询功能模块中管理员可以完成查询当前在线、非在线用户列表，查询现有用户，查询用户合法、非法登陆、拨号认证的系统日志，以及拨号用户的计费信息统计等功能：

★ **在线用户** － 查询当前在线用户列表。

★ **非在线用户** － 查询当前非在线用户列表。

★ **用户操作日志** － 查询管理员对用户的操作记录。

★ **用户登录日志** － 查询各级用户 Web 方式登陆，以及认证用户拨号认证的日志信息。

★ **非法登录日志**－ 查询各级用户 Web 方式登陆，以及认证用户拨号认证过程中发生错误的日志信息。

★ **计费信息** － 统计用户登陆次数和在线时长的信息。

★ **系统日志** － 查询系统操作记录，管理员还可以导出该日志到本地磁盘存储，导出格式为.CSV，便于用户导入至 EXCEL 或其他数据库中。

2.7 历史信息

数据存储分三种方式：当前库、历史库、文件，当前库存放当前处理的数据，默认存放周期为 12 个月（完整的 12 个月数据），历史库存放 12 个月以上数据，当数据超过 12 个月后，系统自动将业务数据转移到历史表中，文件存放 36 个月以上的数据，当历史数据超过 36 个月后，系统自动将历史数据转移压缩到文件中。

★ **历史-用户登录日志** － 查询历史拨号认证的日志信息。

★ **历史-非法登录日志**－ 查询历史认证错误的日志信息。

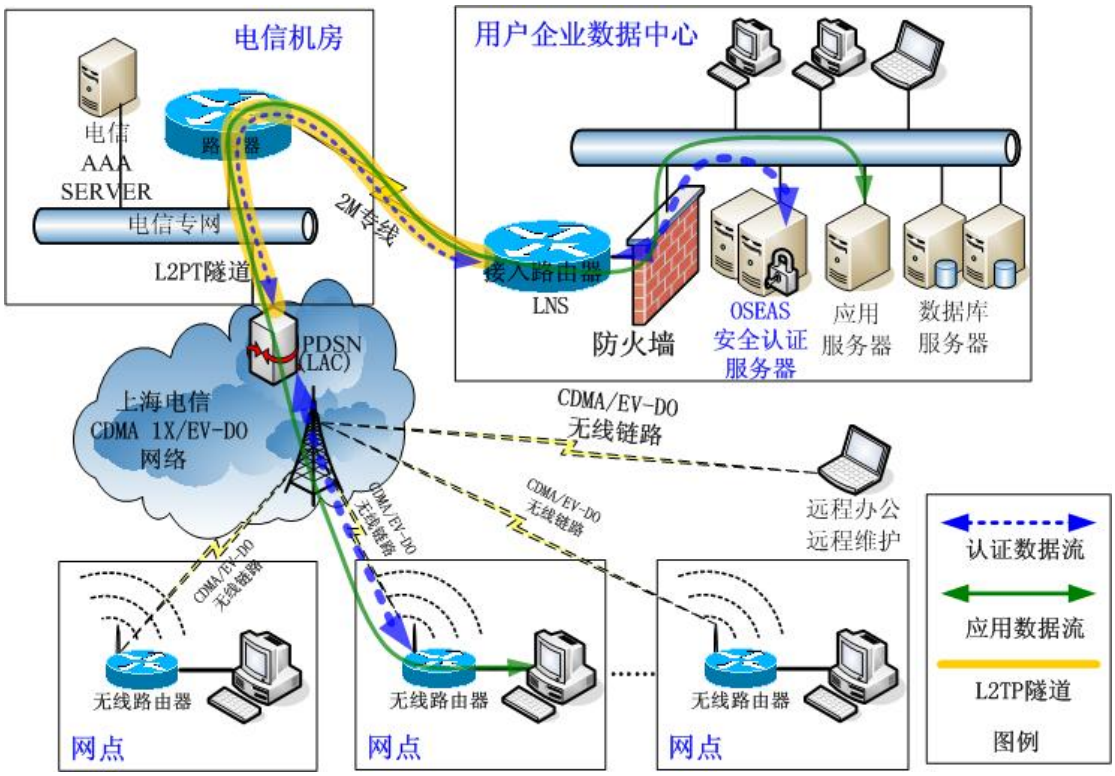
★ **历史-计费信息** － 统计历史登陆次数和在线时长的信息。

★ **历史文件导出** －以文件的方式将历史数据导出，导出格式为.CSV。

第3章. 典型应用场景介绍

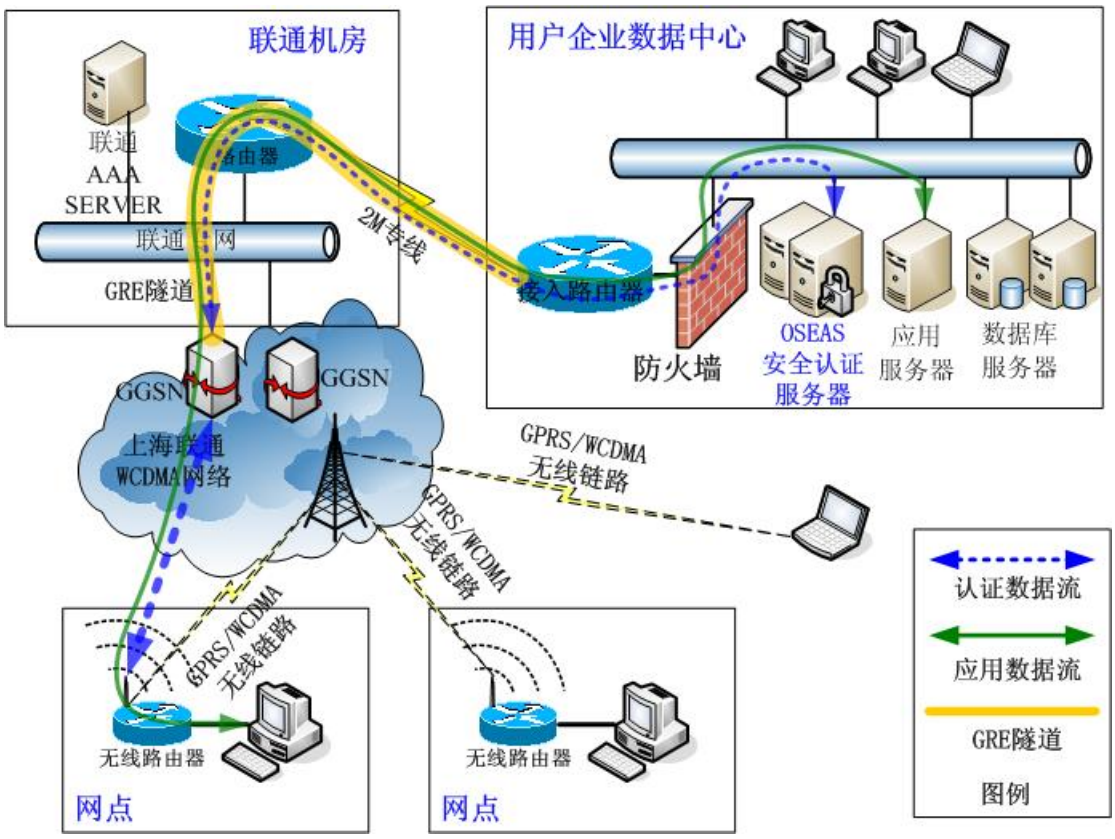
3.1 基于 CDMA 1X / EV-DO VPDN 接入的安全认证

认证服务器部署要求：认证服务器认证端口正确接入企业网络，和 LNS 路由器可以不在一个网段，但两者间必须路由可达，认证和记账端口（默认为 1812,1813）数据通讯正常。



3.2 基于 WCDMA / GPRS APN 接入的安全认证

认证服务器部署要求：认证服务器认证端口正确接入企业网络，和联通 GGSN 间的路由可达，认证和记账端口（默认为 1812,1813）数据通讯正常。



3.3 典型用户

1. 金融：

- 建设银行上海分行
- 建设银行宁波分行
- 交通银行上海分行
- 交通银行太平洋信用卡中心

应用：ATM 接入，2G/3G 无线 POS，离行业务终端无线接入；

2. 政府及事业单位：

- 上海市公安局交警总队
- 上海市无线电管理局
- 国家海洋局东海预报中心（上海、宁波、温州、厦门、宁德）
- 国家海洋局技术中心
- 四〇五
- 上海市医保中心
- 民航华东空管局

应用：OA，远程监测点数据传输，远程维护；视频传输，医保异地结算；

3. 连锁及物流

- 捷强连锁
- 台湾贸宏

应用：连锁门店接入，货运车辆（视频、GPS 定位、门锁）实时监控；

第4章. 技术支持

地址：上海市长宁区定西路1279号4C

邮编：200050

传真：(021)62519185

客户服务：(021)62516676

邮件支持：support@optirise.com

公司网站：http://www.optirise.com

附录 1 技术规范

物理属性	
电源	220V/50Hz 250W(最大)
机型	标准1u机架式机箱
长度/宽度/高度(cm)	482.6mm（长）×425mm（宽）×43.6mm（高） 500mm（长）×425mm（宽）×88mm（高）
重量(Kg)	6.12
相对湿度	10-90%@40摄氏度，非冷凝
工作温度	0—45摄氏度
非工作温度	-20—65摄氏度
网络接口	
4个 10/100/1000M 自适应	
系统主要功能	
认证	用户名、密码＋IMSI号双因素绑定认证
授权	可为拨号用户分配指定的IP地址 可为双LNS结构下经由不同LNS发起认证的ppp用户对应分配不同的IP地址
记账	记录认证请求的时间和用户在线时长等信息
防火墙功能	内置
支持的管理方式	WEB Console（串口管理）
强大的日志系统	支持
管理帐号分级	支持
自定义服务	支持
批量处理功能	支持，批量增加修改拨号用户账户
性能	
最大用户数量	5000/50000
最大并发认证数(个/秒)	200/500