方案设计说明书

秘级：

**云平台广告路由NGY5系统**

**项目方案书**

REV.0.1

|  |  |  |  |
| --- | --- | --- | --- |
| 文档编号： | REV.3.1 | 项目名称： | 云平台广告路由NGY5系统 |
| 编 写： |  | 编写日期： | 2018-06-25 |
| 审 核： |  | 审核日期： |  |

**目 录**

[方案设计说明书 1](#_Toc307175225)

[第一章 概 述 6](#_Toc307175226)

**[1.1 编写目的](#_Toc307175227)** [6](#_Toc307175227)

**[1.2 编写背景](#_Toc307175228)** [6](#_Toc307175228)

**[1.2.1](#_Toc307175229)** [系统名称及版本号 6](#_Toc307175229)

**[1.2.2](#_Toc307175230)** [任务承接者及实施者 6](#_Toc307175230)

**[1.3 项目内容](#_Toc307175231)** [6](#_Toc307175231)

**[1.4项目目标](#_Toc307175232)** [7](#_Toc307175232)

**[1.5 文档概述](#_Toc307175233)** [7](#_Toc307175233)

**[1.5.1](#_Toc307175234)** [文档结构说明 7](#_Toc307175234)

**[1.5.2](#_Toc307175235)** [电子文档编写工具 7](#_Toc307175235)

**[1.5.3](#_Toc307175236)** [定义说明与符号 7](#_Toc307175236)

**[1.5.4 参考资料](#_Toc307175237)** [8](#_Toc307175237)

[第二章 基础理论和原理分析 10](#_Toc307175238)

**[2.1](#_Toc307175239)** [视频数据的3G网络传输子系统原理方框图 10](#_Toc307175239)

**[2.2](#_Toc307175240)** [基础理论与原理分析 10](#_Toc307175240)

**[2.2.1](#_Toc307175241)**[视频数据的3G网络传输子系统的工作原理 10](#_Toc307175241)

**[2.2.2](#_Toc307175242)**[系统设计涉及的基本理论 10](#_Toc307175242)

[2.2.2.1 实时视频传输的特点 10](#_Toc307175243)

[2.2.2.2 无线移动信道的特点 10](#_Toc307175244)

[2.2.2.3 Linux操作系统 11](#_Toc307175245)

[2.2.2.4 传输协议 12](#_Toc307175246)

[2.2.2.4.1传输协议TCP 12](#_Toc307175247)

[2.2.2.4.2传输协议UDP 12](#_Toc307175248)

[2.2.2.4.3 实时传输协议RTP 13](#_Toc307175249)

[2.2.2.4.4实时传输控制协议RTCP 15](#_Toc307175250)

[2.2.2.5 拥塞控制 18](#_Toc307175251)

[2.2.2.5.1拥塞控制基本原理 18](#_Toc307175252)

[2.2.2.5.2 TCP的拥塞控制 20](#_Toc307175253)

[2.2.2.6 SPI 20](#_Toc307175254)

[2.2.2.6.1 SPI简介 20](#_Toc307175255)

[2.2.2.6.2 SPI通信原理 20](#_Toc307175256)

[2.2.2.6.3 S3C2440的SPI通信模块 21](#_Toc307175257)

[2.2.2.7 通信模块驱动 23](#_Toc307175258)

[2.2.2.7.1 引言 23](#_Toc307175259)

[2.2.2.7.2 USB设备基础知识 24](#_Toc307175260)

[2.2.2.7.3 USB设备驱动设计 26](#_Toc307175261)

[第三章 方案设计 30](#_Toc307175262)

**[3.1 总体方案](#_Toc307175263)** [30](#_Toc307175263)

**[3.1.1](#_Toc307175264)** [系统总体软件设计 30](#_Toc307175264)

**[3.1.2](#_Toc307175265)** [整体软件设计流程说明 31](#_Toc307175265)

**[3.2 SPI模块方案设计](#_Toc307175266)** [32](#_Toc307175266)

[3.2.1 使用SPI模块的原因 32](#_Toc307175267)

**[3.2.2](#_Toc307175268)** [S3C2440的SPI模块 32](#_Toc307175268)

**[3.3](#_Toc307175270)** [RTP数据包方案设计 35](#_Toc307175270)

[3.3.1 选择UDP协议的原因 35](#_Toc307175271)

[3.3.2 选择RTP/RTCP协议的原因 35](#_Toc307175272)

**[3.4](#_Toc307175273)** [信道轮转调度方案设计 36](#_Toc307175273)

[3.4.1 信道网络状态信息维护 36](#_Toc307175274)

[3.4.2信道轮转调度策略 36](#_Toc307175275)

**[3.5](#_Toc307175276)** [通信驱动程序模块方案设计 37](#_Toc307175276)

[3.4.1简介 37](#_Toc307175277)

[3.4.2方案选择 37](#_Toc307175278)

[3.4.3 EM770 37](#_Toc307175279)

[3.4.4 TCP/IP数据传输的实现 38](#_Toc307175280)

[3.4.5 通信模块接口 38](#_Toc307175281)

[结 束 语 38](#_Toc307175282)

**[文档修订记录](#_Toc307175283)** [39](#_Toc307175283)

**第一章 概 述**

**1.1 编写目的**

**本技术方案主要是针对云平台广告NGY5系统软件总体方案书，主要描述基于WIFI网络PORTAL认证技术以及AAA认证计费技术实现各种广告推送实现商业WIFI各种价值的系统，并对需求范围的界定和主要实现技术方案的说明。**

**预期读者：广州捷轻科技有限公司、黄雅莉、刘开杰、黄伟恩、欧博、李运灵、陈宏钦、陈俊晓、陈梓俊、刘晓柔。**

**1.2 编写背景**

**近一两年，以智能手机、平板电脑为代表移动智能终端快速普及，并且Wi-Fi已成为移动智能终端的标准配置，各种移动智能终端应用软件也日益依赖无线互联网，因此，使用人群对无线接入互联网的需求在进入“移动智能终端时代”后大大增加，虽然3G技术提供了移动互联网接入的手段，但3G基站并不能支撑大用户量并发，WLAN建设成本低速度快，成为性价比最高的无线互联网接入技术。**

**越来越多的商业用户在营业区域都进行了无线覆盖，以向自己的最终用户提供便利的无线接入互联网服务，把无线接入互联网服务作为吸引客户人流，为最终用户提供便利，提升商户服务体验水平的措施之一。**

Wi-Fi运营已进入免费时代，但免费不等于没有可持续盈利的商业模式，Wi-Fi的盈利点应从提供互联网服务转变为利用Wi-Fi促进企业的主营业务，Wi-Fi运营也需要从只关注终端用户体验，转变为同时关注无线覆盖区域所在企业的需求和体验。Portal平台就是实现以上转变的重要载体和平台。

**1.2.1** 系统名称及版本号

系统名称：云平台广告路由NGY5系统

版本号：REV3.1

**1.2.2** 任务承接者及实施者

项目的经理：黄伟恩

本子系统详细设计的负责人及工作人员名单：黄雅莉、**欧博、李运灵、陈宏钦、陈俊晓、陈梓俊、刘晓柔。**

**1.3 项目内容**

本项目是基于原来已经在生产系统上线运作的云平台NGY5系统上进行开发，分别实现以下功能：

**1.3.1 完善以下功能**

1） 云平台后台各种菜单和按钮的重新排放；

2） 完善云平台的代理商充值运营功能。

**1.3.2 新增以下功能**

1）新增云平台与原厂设备的RCI协议V4.0版本，尽量减少云平台和设备之间的交互此时，缩短设备的处理时间；

2）新增微信广告机管理功能

3）新增WIFI强制推送广告机以及对应的云平台管理功能

**1.4项目目标**

本项目需要达到的目标如下：把云平台NGY5系统改造成互联网用户（非专业用户）可直观使用的WIFI广告推送平台系统，并新增集成各种强制WIFI推送功能为一身的强大推送系统。使其实现集WIFI广告、微信吸粉、探针数据等商业WIFI应用为一身的广告推送平台服务。

**1.5 文档概述**

**1.5.1** 文档结构说明

本文档从基本理论知识,原系统现状,方案设计三方面介绍了云平台NGY5系统方案的软件操作、基础理论、工作原理及实现。

**1.5.2** 电子文档编写工具

文档编写为word2003。图形采用Visio2003绘制。

**1.5.3** 定义说明与符号

|  |  |
| --- | --- |
| BRAS | 宽带远程接入服务器 |
| DHCP | 动态主机设置协议 |
| DNS | 域名系统 |
| NAI | 网络访问标识符 |
| RADIUS | 远程用户拨号认证系统 |
| AAA | 认证，授权，记账 |
| SSL | 数据通讯安全套接层 |
| CHAP | 点对点询问握手认证协议 |
| PAP | 点对点密码认证协议 |
| Portal Server | 门户网站。推送认证页面，接收WLAN用户的认证信息，向AC发起用户认证请求。以及用户下线通知 |

。

**1.5.4 参考资料**

**[1] IEEE Std.802.11, 1999 Edition[ISO/IEC 8802-11: 1999], Standards for Local and Metropolitan Area Networks-Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications.**

**[2] IEEE Std.802.11b, 1999 Edition[ISO/IEC 8802-11: 1999], Standards for Local and Metropolitan Area Networks-Part11:Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications: High-Speed Physical layer Extension in the 2.4GHz Band.**

**[3] IEEE P802.11f, 2001, Recommended Practices for Multi-Vendor Access Point Interoperability via Inter-Access Point Protocol across Distribution Systems supporting IEEE P802.11 operation.**

**[4] IEEE 802.11i, 2001, Standards for Local and Metropolitan Area Networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Medium Access Method (MAC) Security Enhancements.**

1. **基础理论和原理分析**

**2.1 RADIUS 认证计费功能**

本系统的PORTAL认证模块是围绕着RAIDUS认证计费功能而展开，首先需要在云平台上部署RADIUS认证计费服务，才能和各个厂家的BRAS设备进行认证计费交互操作，并且记录用户的上网信息数据。

**2.1.1 简介**

RADIUS是一种C/S结构的协议，它的[客户端](http://baike.baidu.com/view/930.htm" \t "https://blog.csdn.net/jiayanhui2877/article/details/_blank)最初就是[NAS](http://baike.baidu.com/view/56335.htm" \t "https://blog.csdn.net/jiayanhui2877/article/details/_blank)（Net Access Server）[服务器](http://baike.baidu.com/view/899.htm" \t "https://blog.csdn.net/jiayanhui2877/article/details/_blank)，现在任何运行RADIUS客户端软件的计算机都可以成为RADIUS的客户端。RADIUS协议认证机制灵活，可以采用[PAP](http://baike.baidu.com/view/262971.htm" \t "https://blog.csdn.net/jiayanhui2877/article/details/_blank)、[CHAP](http://baike.baidu.com/view/64309.htm" \t "https://blog.csdn.net/jiayanhui2877/article/details/_blank)或者Unix登录认证等多种方式。RADIUS是一种可扩展的协议，它进行的全部工作都是基于Attribute-Length-Value的向量进行的。RADIUS也支持厂商扩充厂家专有属性。　　由于RADIUS协议简单明确，可扩充，因此得到了广泛应用，包括普通电话上网、[ADSL](http://baike.baidu.com/view/659.htm" \t "https://blog.csdn.net/jiayanhui2877/article/details/_blank)上网、小区宽带上网、IP电话、[VPDN](http://baike.baidu.com/view/333397.htm" \t "https://blog.csdn.net/jiayanhui2877/article/details/_blank)（Virtual Private Dialup Networks，基于拨号用户的虚拟专用拨号网业务）、移动电话预付费等业务。最近IEEE提出了[802.1x](http://baike.baidu.com/view/310804.htm" \t "https://blog.csdn.net/jiayanhui2877/article/details/_blank)标准，这是一种基于[端口](http://baike.baidu.com/view/1075.htm" \t "https://blog.csdn.net/jiayanhui2877/article/details/_blank)的标准，用于对[无线网络](http://baike.baidu.com/view/5030.htm" \t "https://blog.csdn.net/jiayanhui2877/article/details/_blank)的接入认证，在认证时也采用RADIUS协议。

**2.1.2 基本工作原理**

用户接入NAS，NAS向[RADIUS服务器](http://baike.baidu.com/view/2240873.htm" \t "https://blog.csdn.net/jiayanhui2877/article/details/_blank)使用Access-Require[数据包](http://baike.baidu.com/view/25880.htm" \t "https://blog.csdn.net/jiayanhui2877/article/details/_blank)提交用户信息，包括用户名、密码等相关信息，其中用户密码是经过MD5加密的，双方使用共享[密钥](http://baike.baidu.com/view/934.htm" \t "https://blog.csdn.net/jiayanhui2877/article/details/_blank)，这个密钥不经过网络传播；RADIUS服务器对用户名和密码的合法性进行检验，必要时可以提出一个Challenge，要求进一步对用户认证，也可以对NAS进行类似的认证；如果合法，给NAS返回Access-Accept数据包，允许用户进行下一步工作，否则返回Access-Reject数据包，拒绝用户访问；如果允许访问，NAS向RADIUS服务器提出计费请求Account-Require，RADIUS服务器响应Account-Accept，对用户的计费开始，同时用户可以进行自己的相关操作。　　RADIUS还支持代理和漫游功能。简单地说，代理就是一台服务器，可以作为其他RADIUS服务器的代理，负责转发RADIUS认证和计费数据包。所谓漫游功能，就是代理的一个具体实现，这样可以让用户通过本来和其无关的RADIUS服务器进行认证，用户到非归属运营商所在地也可以得到服务，也可以实现虚拟运营。　　RADIUS服务器和NAS服务器通过UDP协议进行通信，RADIUS服务器的1812端口负责认证，1813端口负责计费工作。采用UDP的基本考虑是因为NAS和RADIUS服务器大多在同一个[局域网](http://baike.baidu.com/view/788.htm" \t "https://blog.csdn.net/jiayanhui2877/article/details/_blank)中，使用UDP更加快捷方便，而且UDP是无连接的，会减轻RADIUS的压力，也更安全。　　RADIUS协议还规定了重传机制。如果NAS向某个RADIUS服务器提交请求没有收到返回信息，那么可以要求备份RADIUS服务器重传。由于有多个备份RADIUS服务器，因此NAS进行重传的时候，可以采用轮询的方法。如果备份RADIUS服务器的密钥和以前RADIUS服务器的密钥不同，则需要重新进行认证。

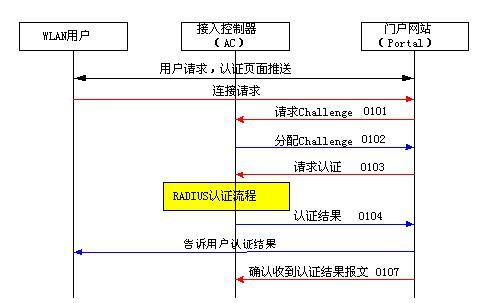
**2.2 PORTAL认证协议**

本系统的PORTAL认证模块和其他BRAS厂家（华三、信瑞、华为、中兴、锐捷等）进行认证交互时，需要通过PORTAL协议进行交互操作，此协议在《中国移动WLAN业务PORTAL协议规范2.0》基础上进行了部分扩展。

**2.2.1用户上线流程**

上线流程完成用户账号的认证，并把认证结果通知Portal Server，Portal server将会通知WLAN用户并且显示相应的认证结果。

用户上线Chap认证流程，如图：



1. 用户访问网站，经过AC重定向到Portal Server，Portal Server推送认证页面；
2. 用户填入用户名、密码，提交页面，向Portal Server发起连接请求；
3. Portal Server向AC请求Challenge；
4. AC分配Challenge给Portal Server；
5. Portal Server向AC发起认证请求；
6. 而后AC进行RADIUS认证，获得RADIUS认证结果；
7. AC向Portal Server送认证结果；
8. Portal Server将认证结果填入页面，和门户网站一起推送给客户；
9. Portal Server回应确认收到认证结果的报文。

**2.2.2报文格式与字段说明**

协议包采用固定长度头加可变长度的属性字段组成，属性字段采用TLV格式，具体如图所示。



报文类型TYPE对应关系如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **值** | **方向** | **含义** |
| REQ\_CHALLENGE | 0x01 | Client----->Server | Portal Server 向AC设备发送的请求Challeng报文 |
| ACK\_CHALLENGE | 0x02 | Client<-----Server | AC设备对Portal Server请求Challeng报文的响应报文 |
| REQ\_AUTH | 0x03 | Client----->Server | Portal Server向AC设备发送的请求认证报文 |
| ACK\_AUTH | 0x04 | Client<-----Server | AC设备对Portal Server请求认证报文的响应报文 |
| REQ\_LOGOUT | 0x05 | Client----->Server | 若ErrCode字段值为0x00，表示此报文是Portal Server向AC设备发送的请求用户下线报文；若ErrCode字段值为0x01，表示该报文是Portal Server发送的超时报文，其原因是Portal Server发出的各种请求在规定时间内没有收到响应报文。 |
| ACK\_LOGOUT | 0x06 | Client<-----Server | AC设备对Portal Server请求下线报文的响应报文 |
| AFF\_ACK\_AUTH | 0x07 | Client----->Server | Portal Server对收到的认证成功响应报文的确认报文； |
| NTF\_LOGOUT | 0x08 | Server --> Client | 用户被强制下线通知报文 |
| REQ\_INFO | 0x09 | Client --> Server | 信息询问报文 |
| ACK\_INFO | 0x0a | Server --> Client | 信息询问的应答报文 |

其中报文属性ATTR\_TYPE对应关系如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **Attr(属性字段)** | **AttrType** | **属性值长度** | **属性含义** |
| UserName | 0x01 | <=32 （可变） | 用 户 名，具体为：  “用户名”＋“@”+“域名” |
| PassWord | 0x02 | <=16（可变） | 用户提交的明文密 码 |
| Challenge | 0x03 | 16（固定） | Chap方式加密的魔 术 字 |
| ChapPassWord | 0x04 | 16（固定） | 经过Chap方式加密后的密码 |

**2.2.3 PORTAL页面参数字段说明**

当AC实现强制PORTAL功能时，要求在强制PORTAL URL中包含以下参数：

| 参数名称 | 参数取值 | 参数说明 | 作用阶段 | 举例 |
| --- | --- | --- | --- | --- |
| wlanuserip | 十进制的字符串格式  网段在前，主机在后 | WLAN用户的私网地址，是认证Portal与AC之间判别WLAN用户的身份识别码 | 重定向认证页面请求时 | wlanuserip=10.1.2.34 |
| wlanusername | IMSI@SIM格式的字符串格式 | WLAN用户的用户名 | 重定向门户网站页面请求时 | [wlanusername=IMSI@SIM](mailto:wlanusername=13810910001@SIM) |
| wlanacname | 十进制的字符串格式 | wlanacname=ACN**.**CTY**.**PRO**.**OPE，属性名为严格小写，属性值为唯一的AC名称。 | 重定向认证页面请求时 | wlanacip= ACN**.**CTY**.**  PRO**.**OPE |

**2.3 OPENWRT系统**

本系统的云平台管理负责RADIUS认证、PORTAL页面管控以及网络设备管控等功能，而最基础的用户认证、广告推送、微信吸粉、探针探测、设备管理等，都需要一个自主研发的基础网络设备中进行嵌入式开发才能实现。

在网络设备的嵌入式开发中，OPENWRT是一个开源并且广泛兼容各种网络设备的Linux系统，我们将再次系统的基础上进行进一步的嵌入式开发实现各种功能。

**2.3.1 简介**

OpenWrt 可以被描述为一个嵌入式的 Linux 发行版，（主流路由器固件有 dd-wrt,tomato,openwrt三类）而不是试图建立一个单一的、静态的系统。OpenWrt的包管理提供了一个完全可写的文件系统，从应用程序供应商提供的选择和配置，并允许您自定义的设备，以适应任何应用程序。

对于开发人员，OpenWrt 是使用框架来构建应用程序，而无需建立一个完整的固件来支持；对于用户来说，这意味着其拥有完全定制的能力，可以用前所未有的方式使用该设备。

**2.3.2系统特点**

OpenWRT是一个高度模块化、高度自动化的嵌入式Linux系统，拥有强大的网络组件和扩展性，常常被用于工控设备、电话、小型机器人、智能家居、路由器以及VOIP设备中。 同时，它还提供了100多个已编译好的软件，而且数量还在不断增加，而 OpenWrt SDK 更简化了开发软件的工序。

OpenWRT不同于其他许多用于路由器的发行版，它是一个从零开始编写的、功能齐全的、容易修改的路由器操作系统。实际上，这意味着您能够使用您想要的功能而不加进其他的累赘，而支持这些功能工作的linux kernel又远比绝大多数发行版来得新。

如果对 Linux 系统有一定的认识, 并想学习或接触嵌入式 Linux 的话, OpenWRT很适合。 而且OpenWRT支持各种处理器架构，无论是对ARM，X86，PowerPC或者MIPS都有很好的支持。 其多达3000多种软件包，囊括从工具链(toolchain)，到内核(linux kernel)，到软件包(packages)，再到根文件系统(rootfs)整个体系，使得用户只需简单的一个make命令即可方便快速地定制一个具有特定功能的嵌入式系统来制作固件。

一般嵌入式 Linux 的开发过程, 无论是 ARM, PowerPC 或 MIPS 的处理器, 都必需经过以下的开发过程：

1、 创建 Linux 交叉编译环境；

2、建立 Bootloader；

3、移植 Linux 内核；

4、建立 Rootfs (根文件系统)；

5、安装驱动程序；

6、安装软件；

熟悉这些嵌入式 Linux 的基本开发流程后，不再局限于 MIPS 处理器和无线路由器, 可以尝试在其它处理器, 或者非无线路由器的系统移植嵌入式 Linux, 定制合适自己的应用软件, 并建立一个完整的嵌入式产品。

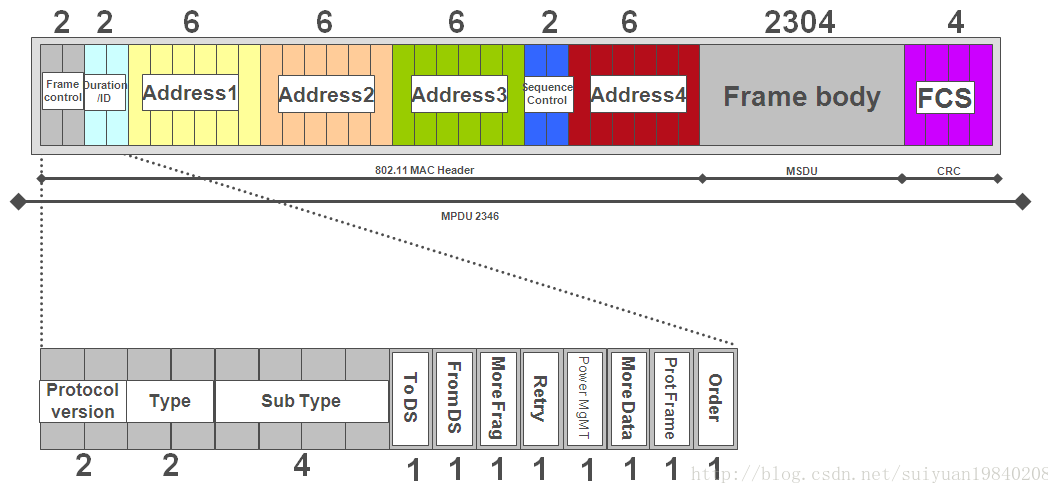


**2.4 WIFI探针技术**

无论是用户人流数据收集，微信强制推送广告机，还是WIFI强制推送广告机，都需要使用WIFI探针技术，也就是需要收集经过当前无线网络设备附近的WIFI客户端的数据，无论该客户是否连上WIFI。

**2.4.1 工作原理**

要深入了解WiFi探针技术，首先先认识WiFi使用的网络协议，WiFi采用的是IEEE802.11协议集，此协议集包含许多子协议。其中按照时间顺序发展，主要有：（1）802.11a，（2）802.11b， （3）802.11g（4）802.11n。在网络通信中，数据被封装成了帧，帧就是指通信中的一个数据块。但是帧在数据链路层传输的时候是有固定格式的，不是随便的封装和打包就可以传输，大小有限制，最小46字节，最大1500字节所以我们必须按照这个规则来封装。下面802.11的帧结构：

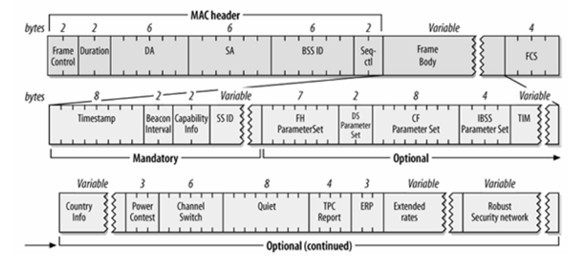


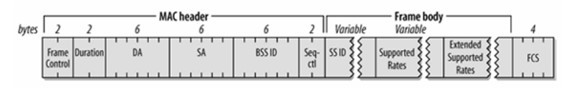
从上面的结构可以知道，前俩个字节为：帧控制字段。  
控制字段的前2bit节为：协议类型，目前此值为：0。

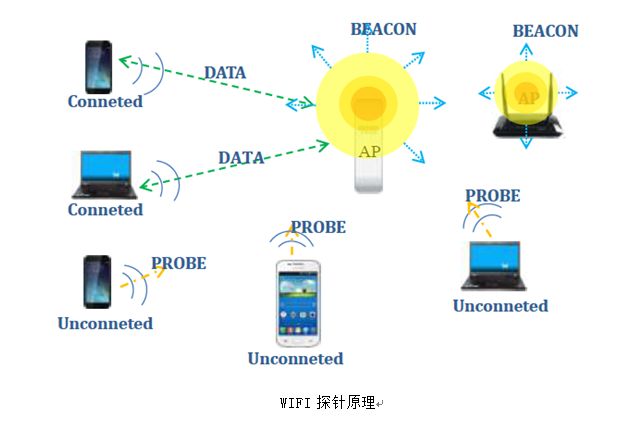
1）控制帧：（Control Frame，例如RTS帧、CTS帧、ACK帧）用于竞争期间的握手通信和正向确认、结束非竞争期等；   
2）管理帧：（Management Frame，例如Beacon帧、Probe Request帧）主要用于STA与AP之间协商、关系的控制，如关联、认证、同步等；   
3）数据帧：（Data Frame，承载数据的载体）用于在竞争期和非竞争期传输数据。

****1、管理帧****

BeaconFrame：信标帧，是相当重要的维护机制，主要来宣告某个AP网络的存在。定期发送的信标，可让移动WiFi设备得知该网络的存在，从而调整加入该网络所必要的参数。在基础网络里，AP必须负责发送Beacon帧，Beacon帧所及范围即为基本服务区域。 在基础型网络里，所有沟通都必须通过接入点，因此WiFi设备不能距离太远，否则无法接收到信标。下图是帧格式：

**[](http://s4.51cto.com/wyfs02/M02/85/75/wKioL1ekEkTTNlYwAACVr9Go7hg570.jpg" \t "https://blog.csdn.net/isentech/article/details/_blank)**  
****2、管理帧Probe Request：****

探测请求帧，WiFi设备将会利用Probe Request帧，扫描所在区域内目前有哪些802.11网络。下图是帧格式： [](http://s1.51cto.com/wyfs02/M00/85/75/wKiom1ekEnqQI5jTAAA5PFjvDd4941.jpg" \t "https://blog.csdn.net/isentech/article/details/_blank)****3、数据帧：****

Data数据帧，当接入点要送出一个帧给WiFi设备但是不必确认之前所传送的信息时，就会使用标准的数据帧。标准的数据帧并不会征询对方是否有数据待传，因此不允许接收端传送任何数据。无竞争周期所使用的纯数据（Data-Only)帧和无竞争周期所使用的数据帧完全相同。看了以上的网络知识，我们现在说说WiFi探针是怎么工作的，还是先看张图： [](http://s3.51cto.com/wyfs02/M00/85/75/wKioL1ekErbwBCRqAAFxVHuYQ24766.png" \t "https://blog.csdn.net/isentech/article/details/_blank)  
就像图中描述的一样，我们的WiFi探针其实就是一个AP，它定时的向自己的四周广播发送Beacon帧，用来通知附近的WiFi设备，AP是存在的，（好比它一直在向周围喊着，我在这里，大家快来连接我啊）。 我们的WiFi设备，手机，平板电脑等，也不停的发送着probe帧，去寻找附近可用的AP。在probe帧的介绍中就我们可以看到probe帧包含了设备的mac地址，当我们的AP接收到probe帧之后就获取了这个设备的MAC地址，而这个AP就是我们的WIFI探针。因此只要在WiFi探针覆盖区域内的设备打开着WiFi，探针就能收集到他的MAC地址。

1. **系统现状**

**3.1 云平台系统**

**3.1.1 系统总体框架**



* 上网用户接入到移动的BRAS设备，或者原厂网络设备，打开浏览器输入网址，可以看到宽带接入系统推送的认证页面；
* 用户登录后，网络设备把请求发送到认证计费模块进行认证计费操作；
* 设备管理员登录到后台的设备管理模块，对网络设备进行查看和管理操作；
* 集团客户管理员登录到PORTAL服务管理系统，对上网用户账号、PORTAL页面内容进行统一管理；
* 业务系统、短信系统、APP系统与接口模块进行对接，处理各种业务功能。

**3.1.2 系统模块划分**



* 该系统由 设备管理模块、PORTAL页面推送模块、RADIUS认证计费模块和后台管理模块组成。

**3.1.3 系统已经实现的功能点**

**3.1.3.1 区域节点管理**

* 系统支持区域管理，区域下可以创建子区域或者集团客户节点。
* 每个区域和节点都可以创建管理员，该管理员只能看到对应区域下的所有子区域以及

对应的集团客户节点。

* 区域和节点支持树形结构查看，支持展开/搜索/添加/删除等操作。
* 区域上可以设置某些特定规则，系统会自动把规则应用到其下以及所有子区域的节点上。

**3.1.3.2 与其他BRAS设备的PORTAL认证功能**

* 系统支持配置参数，生成PORTAL协议与RADIUS协议的配置联调文件给BRAS设备进行参数配置。
* 系统支持分析BRAS重定向的URL地址，并在用户登录时，使用PORTAL协议与BRAS设备进行交互，实现方通用户上网的操作。
* 系统支持与BRAS设备进行RADIUS认证计费报文交互，记录用户的上网信息。
* 系统支持一键登录、二次登录、密码认证、账号密码认证、手机认证方式。

**3.1.3.3 与原厂设备的PORTAL认证功能**

* 云平台与原厂设备系统使用TCP连接的扩展PORTAL协议进行认证操作。
* 除了上面描述的几种认证方式外，云平台在原厂网络设备下还支持微信连WIFI登录、微信二维码扫描登录。
* 系统支持与原厂设备进行RADIUS认证计费报文交互，记录用户的上网信息。
* 系统支持与原厂设备下的用户进行MAC无感知认证功能，用户获取dhcp报文时便可以实现自动二次认证功能。

**3.1.3.4 设备管理功能**

* 云平台可以在不同集团客户下添加、管理已经授权的原厂设备。
* 云平台可以编辑、查看原厂设备的备注、位置、地图信息。
* 云平台可以随时查看原厂设备的当前状态，包括是否在线、当前IP、MAC、地址，当前无线配置信息等等。
* 云平台可以进一步查看原厂设备的系统状态，包括CPU、内存、空间等，并对设备进行重启、命令等操作。
* 云平台可以对整个集团客户所有网络设备进行统一配置操作，包括统一修改SSID名称和密码等等。
* 云平台可以对原厂设备进行远程管理，包括远程网页操作、远程telnet调试等等。

**3.1.3.5 用户管理功能**

* 系统支持对各种用户组进行统一设置，包括手机用户组、微信用户组、普通用户组等等。
* 系统支持对用户信息、认证条件、计费条件进行设置，其中认证条件包括用户密码、同用限制、接入时段、绑定MAC列表等等；计费条件包括期限计费、按实际使用时长计费、按每次最长使用时间计费等等。
* 系统支持用户的增删查改操作，支持对用户进行停机或者复机操作。支持批量添加和批量修改用户。

**3.1.3.6 用户上网记录以及登录记录查询功能**

* 分页查看所有在线的用户或者历史用户上网信息，每条信息包括如下属性：

帐号、用户IP、用户MAC、上线时间、计费时长、下行流量、上行流量、网络设备IP、网络设备MAC地址、网络设备标识、网络设备端口标识、所在区域

* 可以根据区域、账号、用户IP、用户MAC、网络设备IP等参数进行查询操作
* 可以对任意在线用户记录执行“强制下线”操作，此操作会把相应信息发到Radius的下线模块进行处理

**3.1.3.7 设备MAC白名单以及主机白名单功能**

* 可以设置设备的MAC白名单列表，使得白名单对应的设备客户端无需进行认证即可直接上网。
* 可以设置域名白名单列表，使用户无需进行登录认证操作，即可访问的此域名列表对应的主机时。
* 系统预支部分域名列表到快速配置按钮中，例如“微信”、“支付宝”，管理员可以直接使用此快速按钮自动添加相应域名列表到白名单列表中。
* 当白名单域名产生变化时，系统会自动把列表同步到在线设备中。

**3.1.3.8 用户套餐以及营销充值功能**

* 用户套餐模型
  + 为每个上网帐号新增可用余额属性，并对此属性的修改新增日志记录。
  + 可以定义用户的套餐属性，包括套餐价格、套餐限速参数。
  + 可以为用户指定相应套餐，其用户的使用期限则按照套餐加个进行计算。
  + 用户在凌晨时间段按照加个扣减用户余额
* 用户充值模型
  + 每个套餐可以对应多个充值选项，填写相关的充值/赠送金额
  + 用户可以选择使用微信支付/支付宝方式进行充值操作
  + 系统可以展现并导出所有用户的充值记录，包括订单号/用户名/充值金额/套餐内容等等

**3.1.4 系统需要优化或新增功能点**

**3.1.4.1 系统各个菜单和界面的图表、排位、文字等优化布局**

系统原来的设计是给移动/电信的运营商使用，其菜单、设计风格均按照运营商后台管理人员的习惯进行设计。现在系统需要改为适合互联网销售，使用对象会改为企业网络管理员使用，因此很多专业名次、菜单和文字都需要经过适当修改。

**3.1.4.2 设备管理RCI 新版本的对接操作**

系统原来使用RCI管理协议，此协议的最大特点是Linux命令交互驱动，这样会大大降低设备的适用范围，并且会添加太多交互次数，延缓设备的操作时间。

新版的RCI协议，实在旧版的基础上，尽量去除Linux命令交互的影响，采用配置下发、虚拟指令的方式代替原来的Linux命令方式，这样可以增加RCI协议的适用范围，并大幅度减少命令交互的次数，提高设备的管理效率。

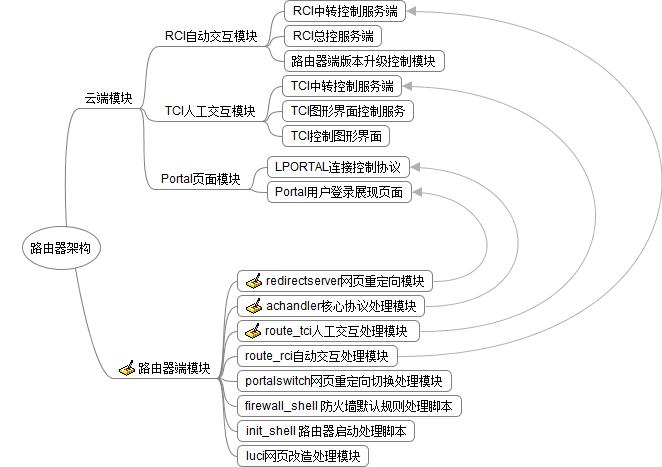
**3.1.4.3 完善云平台的代理商充值运营功能**

**3.1.4.4 完善微信连WIFI的强制关注功能**

**3.1.4.5 管理微信广告机和WIFI强推广告机**

**3.2 嵌入式系统**

**3.2.1系统功能模块**



**3.2.2 系统已经实现的功能点**

**3.2.2.1 路由器模式与AP模式一键切换功能**

**3.2.2.2 多VLAN划分功能**

**3.2.2.3 认证计费功能**

**3.2.2.4 统一管控功能**

**3.2.2.5 HTTP、HTTPS重定向功能**

**3.2.2.6 微信连WIFI以及二维码对接功能**

**3.2.2.7 基于HTTP重定向的域名进行白名单功能**

**3.2.2.8 WIFI探针功能**

**3.2.3 系统需要优化或新增功能点**

**3.2.3.1 支持RCI 4.0 快速连接配置功能**

**3.2.3.2 支持本地化网络规则自定义功能**

目前设备的限速规则、MAC白名单规则、域名白名单规则、异常下线时长等都只能从云平台的RCI接口下发，考虑到以后可能会接入其他系统云平台时候，无法使用RCI接口，则需要用户可以在本地配置这些规则，而并非从云平台获取相应规则。

**3.2.3.3 基于DNS重定向的域名进行白名单功能**

**3.2.3.4 优化目前的WIFI探针功能**

**3.2.3.5 WIFI强推广告机功能**

**3.2.3.6 编写手机APPS连接NGY5设备并收集检测报告**

**第四章 方案设计**

**4.1 云平台优化方案**

**4.1.1 RCI (V4.0)对接方案**

NGY5系统在RCI3.0以及之前的方案，都是使用命令驱动的模式去完成交互操作，也就是云平台直接组装Linux交互指令到设备，然后设备执行指令并把结果告诉平台。这个模式很大程度上上限制了设备的选型以及平台，如果设备并非OPENWRT则无法支持。

因此，必须设计出非命令交互驱动的RCI (V4.0) 交互协议，用以进行认证对接，这个协议具有以下要点：

* 协议使用TCP连接，并且定期进行keepalive的TCP操作；
* 在设备连接初期，设备需要传送所有云平台需要的信息给云平台；
* 云平台一次性提供所有PORTAL协议认证参数、限速参数、白名单参数给设备
* 设备根据云平台提供的参数，调用自己的预置脚本进行处理
* 云平台可以下发各种管控命令，这些命令并非以Linux命令的形式发给设备，其中包括如下命令：
  + - 1. 获取设备的各种运行信息；
    - 2. 设置设备无线的SSID、信道、功率、密码等等；
    - 3. 设置设备的限速状况
    - 4. 修改设备的运行模式 （ROUTER / AP)
    - 5. 修改设备的PORTAL认证模式 （是否进行PORTAL认证）
    - 6. 控制设备连接TELNET代理端口
    - 7. 控制设备打开VPN代理端口

**4.1.2 完善云平台的代理商充值运营功能**

详见《美溪新需求开发文稿n.pptx》

**4.1.3 完善微信连WIFI的强制关注功能**

目前的微信连WIFI强制关注功能，采用的是定期检测用户是否关注，如果未关注则断线，这种明显不够实时性，需要优化此流程。

优化方案如下：

用户选择微信连WIFI =》 系统调用微信连WIFI接口 =》 在接口内判断用户是否已经关注，如果未关注，则不跳转到登录接口，直接返回成功页面 =》 用户选择是否关注 =》用户点击“完成”按钮 =》 跳转到平台预置的完成页面 =》页面判断用户是否已经关注，如果已经关注，则直接调用登录接口 =》如果未关注，则再次发起微信连WiFi

**4.2 嵌入式优化方案**

**结 束 语**

本部分为云平台NGY5系统的一个总体优化方案说明

**文档修订记录**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序 号 | 修改时间 | 修 改 人 | 审 核 人 | 备 注 |
| 1 | 2011-11-07 | 张志浩 |  | 自适应流量控制算法修改 |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 9 |  |  |  |  |
| 10 |  |  |  |  |
| 11 |  |  |  |  |
| 12 |  |  |  |  |
| 13 |  |  |  |  |
| 14 |  |  |  |  |
| 15 |  |  |  |  |