基于Portal的WiFi认证登录系统的详细设计

引言

项目名称

基于Portal的WiFi认证登录系统

项目背景

**近十多年来年，随着信息和科技的高速发展，互联网承载着各种各样的信息，而且信息量非常巨大，人们不但可以从网上获取到大量自己需要的信息，还可以使用互联网，上传自己想要表达的信息，由于大量的需求，产生了一个巨大的市场，所以就使得智能手机、平板电脑为代表移动智能终端快速普及。随着信息的增大，而使用2G、3G、4G的通讯方式去获取大量的网络信息会造成巨大的上网成本，这些上网方式已经满足不了用户对流量的需求，所以WIFI技术就应运而生，WLAN建设成本低速度快，网络流量限制小，成为性价比最高的无线互联网接入技术，因此WiFi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因为WiFi的诞生发展而给用户呈现出更大的信息量，更快的网络速度，极大地祢补了用户对网络流量和速度的需求。然而，随着互联网和计算机科学的继续发展，用户对流量和网速的需求也日益增高。因此，人群对无线接入互联网的需求在进入“移动智能终端时代”后也必将大大增加。**

**由于WLAN的建设成本低，流量无限制，网速相对快，越来越多的公司和商业用户都在一定区域内进行了无线覆盖，以向自己以及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不但可以便利公司的基本运作，还可以为商户的客户提供更多的便利，实在是提高工作效率、提高客户体验的措施之一。**

虽然Wi-Fi运营已进入免费时代，但免费不等于没有其存在的商业价值，Wi-Fi的商业价值与传统服务的商业价值不同，传统服务的商业价值是直接与服务挂钩，但是WiFi的商业价值是给用户提供互联网服务，增强用户的体验感，从而促进企业的主营业务。但是WiFi也有其固有的限制，比如安全因素和人多的情况下，网速会比较慢，所以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，实现服务更有针对性和高效性。Portal平台就是实现以上转变的重要载体和平台，通过portal认证，企业可以更加精确的为自己最终的客户提供互联网服务，此外还可以做一些适当的推广，充分地宣传自己。

项目概述 研究的技术能实现什么、通过什么实现

基于portal的WiFii认证登录系统，区别于传统WiFi输入密码来使用网络的情景，portal认证是通过网页，让用户输入手机号码和验证码来验证登录，然后才获得网络的使用权，portal认证还支持在认证页面上插入广告，并且在认证通过后可以使用户进入特定页面。

项目目的

由于简单的WLAN服务存在安全危险，另外因为更多非潜在用户接入使得WiFi的网络速度下降，甚至无法使用，导致潜在客户的体验感下降，从而影响主流业务，所以WiFi引入portal认证提高网络的安全性，还能提高对潜在客户服务体验感。另外，为了能更有效地宣传本企业，让用户更加充分了解本企业，可以通过WLAN植入本企业的宣传信息等。

文档结构

1. 引言：介绍项目名称、项目提出的背景及其提出的意义，还简述项目内容，介绍项目的目的，最后还对本详细设计文档的内容结构、读者对象、相关术语、以及编写工具做了相关的阐述。
2. 需求分析：可行性分析和业务需求分析
3. 程序设计：程序执行过程的各个模块进行设计
4. 测试：测试功能和性能是否达到要求

读者对象

项目经理、开发工程师、测试工程师

术语

portal协议

电子文档编写工具

Microsoft Office 2016

Microsoft visio 2016

需求分析

可行性分析

技术可行性

经济可行性

操作可行性

法律可行性

业务需求分析

登陆认证

WiFi的微信登陆认证

技术分析

portal

概述

Portal汉译的意思是入口。由于Portal认证主要是在Web浏览器进行，因此Portal认证也被称为Web认证，Portal认证网站一般被称为门户网站。还未通过认证的用户连接进有Portal认证的网络时，系统自动提供用户登录特定Web认证登录网站，用户可以免费访问网站中的指定服务。当用户需要访问互联网中的其它信息时，则必须在门户网站进行认证，只有认证通过后才可以接入互联网，访问其中的资源。

产生背景

传统的网络中，认证技术比较简单，终端用户只要通过简单的认证就可以直接地接入互联网，这样会造成很多不安全的因素，同时也会因为网络资源随意被访问而不利于网络的运营管理，所以为加强网络资源的安全控制和运营管理，对终端用户的访问互联网权限必须给予相关的控制。例如，在一些公共场合、小区或公司的网络接入点，提供接入服务的供应商希望只允许付费的合法用户接入，所以供应商为每个用户提供一个接入网络的账号和密码。另外，一些企业会提供一些内部关键资源给外部用户访问，并且希望经过有效认证的用户才可以访问这些资源。

现有的802.1x和PPPoE等访问控制方式，都需要特定客户端的配合，并且只能在接入层对用户的访问进行控制。

Portal认证技术则提供一种相对灵活的访问控制方式，不需要安装特定的客户端，通过网站认证就可以在接入层以及需要保护的关键数据入口处实施访问控制。

Portal认证过程涉及到了认证客户端（Portal client），Portal服务器

（Portal server），BAS和AAA服务器四个基本要素。

图1 Portal系统组成示意图

z Portal client：Portal组网中发起认证请求的客户端系统，为运行HTTP协议的

浏览器。

z Portal server：Portal组网中接受客户端认证请求的服务端系统，提供免费门

户服务和基于WEB认证的界面，与BAS设备交互认证客户端的身份信息。

z BAS：宽带接入服务器，用于向Portal server重定向HTTP认证请求，并且与

Portal server、AAA服务器交互完成用户的认证/授权/计费功能。

z AAA服务器：认证/授权/计费服务器，与BAS进行交互，对用户进行认证/授

权/计费。

以上四个基本要素的交互过程为：

(1)

(2)

未认证用户访问网络时，在 IE 地址栏中输入一个互联网的地址，那么此

HTTP 请求在经过 BAS 设备时会被重定向到 Portal server 的 Web 认证主页

上；

用户在认证主页/认证对话框中输入认证信息后提交，Portal server 会将用户

的认证信息传递给 BAS；

然后 BAS 与 AAA 服务器通信进行用户认证和计费；

认证通过后，BAS 会打开用户与互联网的通路，允许用户访问互

认证流程

Portal认证有两种认证方式：二层认证方式和三层认证方式。二层认证方式又包括

直接认证方式和二次地址方式。

1. 二层认证方式

二次认证方式下，Portal client与BAS直连，或它们之间只有二层设备存在。

z 直接认证方式

用户通过手工配置或DHCP获取的一个公网IP地址进行认证，在认证通过之前，只

能访问Portal服务器以及设定的免费访问地址，认证通过后可使用此IP地址访问外

部网络。

直接认证流程简单，但由于限制了Portal client只能与BAS通过二层交换设备互

连，降低了组网的灵活性。

z 二次地址方式

用户通过DHCP获取一个私网IP地址进行认证，在认证通过之前，只能访问Portal

服务器以及设定的免费访问地址，认证通过后，释放原有私网IP地址，使用重新分

配的公网IP地址访问外部网络。

二次地址方式流程较为复杂，认证通过之前用户可使用私网IP地址，节省了公网IP

地址，但组网方式不灵活。

2. 三层认证方式

这种认证方式允许Portal client和BAS之间跨接三层转发设备，组网方式灵活。因

为三层认证流程与直接认证方式相同，下面将仅对直接认证方式的认证流程和二次

地址方式的认证流程做详细描述。

直接认证

2. 具体步骤

下面认证流程以CHAP认证为例，对于PAP认证方式，步骤（2）、（3）、（4）

可以省略。

Portal client 通过 HTTP 协议触发认证请求。

Portal sever 收到认证请求后，首先向 BAS 设备发送 Challenge 请求报文，

并启动定时器等待 BAS 设备的响应。如果在一定时间内没有收到 BAS 设备

的回应报文，则重传此报文，若到达最大重传次数仍没有回应，则通知

Portal client 认证失败。

BAS 设备收到 Challenge 请求报文后，检查报文的合法性，对合法的报文进

行响应。

Portal server 收到 Challenge 请求报文的响应报文后，根据 CHAP 算法，计

算 CHAP-PASSWORD，然后向 BAS 设备发送请求认证报文，并启动定时器

等待 BAS 设备的响应。如果在规定的时间内没有收到 BAS 设备的回应报

文，Portal server 会重发一定次数的认证请求报文，当达到最大重传次数时

仍没有回应，则通知用户认证失败。

BAS 设备收到请求认证报文后，首先进行合法性检查，对合法的报文进行认

证处理，即根据认证方式（CHAP）构造 RADIUS 认证请求报文发给

Portal技术白皮书

杭州华三通信技术有限公司 www.h3c.com.cn 第8页, 共12页

RADIUS server，然后开启定时器等待 RADIUS server 的认证回应。如果在

规定的时间内 RADIUS server 无响应，则 BAS 设备向 RADIUS server 重发

一定次数的认证请求报文，当达到最大重传次数时仍没有回应，则认为本次

认证失败。

(6)

(7)

BAS 设备根据认证的结果向 Portal sever 发送认证请求响应报文。

Portal server 根据认证请求响应报文表示的认证结果（成功，失败）通知

Portal client 是否认证成功

二次认证

Portal client 通过 HTTP 协议触发认证请求。

Portal sever 收到认证请求后，首先向 BAS 设备发送 Challenge 请求报文，

并启动定时器等待 BAS 设备的响应。

BAS 设备收到 Challenge 请求报文后，检查报文的合法性，对合法的报文进

行响应。

Portal sever 向 BAS 发送请求认证报文，并启动定时器等待 BAS 设备的回

应。

BAS 设备与 RADIUS server 之间进行 RADIUS 协议报文的交互。

BAS 设备根据认证的结果以及定时器的信息向 Portal server 发送请求认证响

应报文，同时在报文中增加控制信息。若认证成功，则控制信息表示要求

Portal server 通知 Portal client 释放 IP，并重新申请 IP 地址。

Portal server 向 Portal client 发送认证通过报文，收到该报文后，Portal

client 释放原私网 IP 地址，并申请新的公网 IP 地址。

BAS 设备通过 Portal client 发送的免费 ARP 报文可以检测到 Portal client 的

IP 地址的状态，一旦检测到 Portal client 的 IP 地址成功更换成公网 IP 地址，

就向 Portal server 发送用户 IP 地址更换的通知报文，并开启定时器等待地址

更新回应报文。

Portal server 在收到 BAS 的用户 IP 地址更换通知，以及客户端的 IP 地址更

新通知后，向 BAS 发送确认报文，并向客户端进行地址更新确认。如果只收

到一方的报文，Portal server 认为用户 IP 地址没有更新。

BAS 收到的确认报文中携带标识地址切换是否成功的信息，若该信息表示地

址切换成功，则 BAS 向 RADIUS server 发送计费请求，请求上线；如果表

示地址切换失败，则 BAS 会向 Portal server 发送报文来强制用户下线。

下线流程

主动下线

强制下线

802.1x技术

简介

IEEE 802.1X是IEEE制定关于用户接入网络的认证标准，全称是“基于端口的网络接入控制”，属于IEEE 802.1网络协议组的一部分。连接在端口上的用户设备如果能通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法访问局域网中的资源。

802.1X系统为典型的Client/Server结构，包括三个实体：客户端（Client）、设备端（Device）和认证服务器（Server）。客户端是位于局域网段一端的一个实体，由该链路另一端的设备端对其进行认证。客户端一般为一个用户终端设备，用户可以通过启动客户端软件发起 802.1X 认证。客户端必须支持EAPOL。设备端是位于局域网段一端的另一个实体，对所连接的客户端进行认证。设备端通常为支持802.1X 协议的网络设备，它为客户端提供接入局域网的端口，该端口可以是物理端口，也可以是逻辑端口。认证服务器是为设备端提供认证服务的实体。认证服务器用于实现对用户进行认证、授权和计费，通常为 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）服务器。

认证过程如下：

802.1X 认证系统使用 EAP（Extensible Authentication Protocol，可扩展认证协议），来实现客户端、设备端和认证服务器之间认证信息的交换。

z 在客户端与设备端之间，EAP 协议报文使用 EAPOL 封装格式，直接承载于 LAN 环境中。

z 在设备端与 RADIUS 服务器之间，可以使用两种方式来交换信息。一种是 EAP 协议报文由设

备端进行中继，使用 EAPOR（EAP over RADIUS）封装格式承载于 RADIUS 协议中；另一种是 EAP 协议报文由设备端进行终结，采用包含 PAP（Password Authentication Protocol，密码验证协议）或 CHAP（Challenge Handshake Authentication Protocal，质询握手验证协议）属性的报文与 RADIUS 服务器进行认证交互。

优点：  
\*802.1x协议为二层协议，不需要到达三层，而且接入层交换机无需支持802.1q的VLAN，对设备的整体性能要求不高，可以有效降低建网成本。

\*通过组播实现，解决其他认证协议广播问题，对组播业务的支持性好。业务报文直接承载在正常的二层报文上；用户通过认证后，业务流和认证流实现分离，对后续的数据包处理没有特殊要求

缺点：

\*需要特定客户端软件

\*网络现有楼道交换机的问题：由于802.1x是比较新的二层协议，要求楼道交换机支持认证报文透传或完成认证过程，因此在全面采用该协议的过程中，存在对已经在网上的用户交换机的升级处理问题；

\*IP地址分配和网络安全问题：802.1x协议是一个2层协议，只负责完成对用户端口的认证控制，对于完成端口认证后，用户进入三层IP网络后，需要继续解决用户IP地址分配、三层网络安全等问题，因此，单靠以太网交换机＋802.1x，无法全面解决城域网以太接入的可运营、可管理以及接入安全性等方面的问题；

\*计费问题：802.1x协议可以根据用户完成认证和离线间的时间进行时长计费，不能对流量进行统计，因此无法开展基于流量的计费或满足用户永远在线的要求。

PPPoE技术

简介

PPPoE使用Client/Server模型，PPPoE的客户端为PPPoE Client，PPPoE的服务器端为PPPoE Server。PPPoE Client向PPPoE Server发起连接请求，两者之间会话协商通过后，PPPoE Server向PPPoE Client提供接入控制、认证等功能。

第一种方式在设备之间建立 PPP 会话，所有主机通过同一个 PPP 会话传送数据，主机上不用安装 PPPoE 客户端拨号软件，一般是一个企业（公司）共用一个账号（图中 PPPoE Client 位于企业/公司内部，PPPoE Server 是运营商的设备）。

第二种部署方式，PPP 会话建立在 Host 和运营商的路由器之间，为每一个Host 建立一个 PPP 会话，每个 Host 都是 PPPoE Client，每个 Host 一个帐号，方便运营商对用户进行计费和控制。Host 上必须安装 PPPoE 客户端拨号软件。

优点：

\*是传统PSTN窄带拨号接入技术在以太网接入技术的延伸

\*和原有窄带网络用户接入认证体系一致

\*最终用户相对比较容易接收

缺点：

\*PPP协议和Ethernet技术本质上存在差异，PPP协议需要被再次封装到以太帧中，所以封装效率很低

\*PPPoE在发现阶段会产生大量的广播流量，对网络性能产生很大的影响

\*组播业务开展困难，而视频业务大部分是基于组播的

\*需要运营商提供客户终端软件，维护工作量过大

\*PPPoE认证一般需要外置BAS，认证完成后，业务数据流也必须经过BAS设备，容易造成单点瓶颈和故障，而且该设备通常非常昂贵。

与现有的802.1x、PPPoE等认证技术相比，Portal认证技术具有以下优势：

不需要部署客户端，直接使用 WEB 页面认证，使用方便；

可以定制“VLAN+端口+IP 地址池”粒度级别的个性化认证页面，同时可以在 Portal 页面上开展广告业务、服务选择和信息发布等内容，进行业务拓展，实现 IP 网络的运营；

关注对用户的管理，可基于用户名与 VLAN ID/IP/MAC 的捆绑识别来认证，并采用 Portal server 和 Portal client 之间，BAS 和 Portal client 之间定期发送握手报文的方式来进行断网检测；

二次地址方式可以实现灵活的地址分配策略和计费策略，且能节省公网 IP 地址；

三层认证方式可以跨越网络层对用户作认证，可以在企业网络出口或关键数据的入口作访问控制。

程序设计

主程序模块

模块一

模块二

模块三

测试

功能测试

功能点一

功能点二

性能测试

内存泄漏等问题