文章编号：2096-1472(2019)-09-23-05
DOI:10.19644/j.cnki.issn2096-1472.2019.09.007

高校WLAN无感知认证系统的设计与实现

王 玮
(北京石油化工学院网络信息中心，北京 102617)

摘 要：随着高校无线局域网部署的日趋完善，对网络安全以及认证都提出了更高的要求，不仅要给师生提供易操作性的网络体验，还要实现高校校园网授权安全准入原则。本文以北京石油化工学院无线网络为环境，提出了基于无线终端MAC地址和Portal统一门户认证相结合的安全准入策略，可以使得用户“一次认证，永久有效”，无感知接入网络。这一目前最为成熟的认证方式，极大地提高了用户使用无线网络的体验感，加快了高校“智慧校园”的建设进程。

关键词：无线网安全；无感知认证；MAC；Portal
中图分类号：TP393 **文献标识码**：A

Design and Implementation of the WLAN Non-perceptual Authentication System in Colleges and Universities

WANG Wei
(*Network Information Center,Beijing Institute of Petrochemical Technology,Beijing* 102617,*China*)

Abstract: With the increasingly perfect deployment of WLAN in colleges and universities,higher requirements have been put forward for network security and authentication.It is not only necessary to provide easy-to-operate network experience for teachers and students,but also to realize the principle of authorized security access of campus network in colleges and universities.Based on the wireless network of Beijing Institute of Petrochemical Technology,this paper proposes a security access strategy based on the combination of wireless terminal MAC address and Portal unified portal authentication,which can enable users to *Authenticate Once and Get Access Forever* to network.This is the most mature authentication method at present,which greatly improves the user's experience of using wireless network and speeds up the construction process of "smart campus" in colleges and universities.

Keywords:WLAN security;non-perceptual authentication;MAC;Portal

1 引言(Introduction)

随着移动设备在日常生活中的普及，我们希望处理更多的应用是通过移动无线网络来实现的[1]。对于高校来说，校园网的有线、无线的流量比值也逐渐下降，用户使用网络已经不局限于有线环境中，而是利用无线网络的开放性，随时随地方便、快捷地接入网络[2]。无线网络的全面覆盖使得智能无线终端设备摆脱了地点和对象的束缚，极大提升了广大师生工作与生活效率，加快了高校信息化发展。但是，无线网络终端设备的移动性和传输信道的开放性，决定了无线网络在安全性方面有一个天然的弱势，导致干扰和拥塞加剧[3]，数据的传输安全能否得到保障，是无线网络环境下无法避免的问题[4]。这使得接入认证的安全性需求大大提高，而无线局域网的准入认证始终难以避免烦琐的缺点。如何要找到一种统一的认证方案，既能够提高校园网有线、无线接入的安全性，又能够便捷地使用户快速接入校园网，是一个亟待解决的问题。

本文以北京石油化工学院无线网络建设为实施环境，为解决最初方案中断线重连、漫游掉线、二次认证等影响用户使用的问题，提出了一套具有通用性、可广泛推广的较为先进的技术方案，即终端设备MAC地址和认证服务器Portal相结合的用户无感知认证方式，实现了终端设备进入无线环境中零配置自动连入校园网，最大限度地提升了用户体验。

2 认证技术分析(Analysis of authentication technology)

该校在最初无线网络实施的过程中采用了当时主流的WLAN网络接入方式Portal认证。该认证使得用户每次接入无线网时都需要在弹出的Portal页面输入用户名和密码以仅仅获

取校内网的访问权限，如果需要访问互联网还需要经过计费系统的“二次认证”，即一次准入接入校园网，二次准出接入互联网并进行计费。尽管这两次输入的用户名和密码都是一致的，但依然给用户带来很大的麻烦。不仅如此，特别是如今使用无线网络的智能手机、平板电脑等终端设备越来越多，各设备受到浏览器、屏幕尺寸等资源限制，认证系统提供的Portal页面并不能够兼容所有终端浏览器，使得用户认证信息的输入受到各种限制，这些都会让用户的上网体验大打折扣。由此看来，以上问题都出现在安全性认证方面，因此如何简化认证过程，尽可能使认证过程用户无感知化，才是解决用户上网体验的核心问题。

基于MAC地址与Portal页面相结合的认证架构

(1)MAC地址认证

由于无线网的传输介质没有固定的边界，因此无法用类似有线网络的交换机端口那样实现接入认证。

但是，在无线网络中，无线终端和无线控制器(AC)在建立数据传输的通信链路之前，可以用终端唯一的MAC地址进行身份验证，并且MAC地址认证无须安装任何形式的客户端，也无须证书校验，用户完全零操作[5]。这种MAC地址绑定的认证方案需要在终端接入无线网络之前，将用户的个人信息与MAC地址绑定。用户接入无线网络时，认证服务器会获取当前设备的MAC地址，然后根据MAC地址到后台数据库对比用户身份信息，与绑定数据一致则放行，否则拒绝请求。该方案的优点是：即使非法用户获取合法用户的身份信息，也无法登录无线网络，安全性有一定的保障。但是也明显存在以下缺点：庞大的网络用户终端的MAC地址信息搜集十分烦琐；存在非法用户伪造MAC地址的危险，安全性较低。

(2)Portal页面认证

Portal认证技术提供了一种灵活的访问控制方式，不需要安装客户端，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[6]，由Portal服务器强制推送给用户的Web认证页面，以达到身份验证的目的。由于Portal服务器的放置位置非常灵活，可以在接入层、汇聚层、核心上旁挂或者串接，不需要安装认证客户端，方便高效。另外，Portal还可以根据不同的用户推送相关页面如重要通知、纪念活动等。但是，Portal认证也有一些不足：比如Portal认证工作在三层，本身无法获取用户的MAC地址，所以无法实现无感知；对用户的识别也做不到精确，由此导致存在着认证的漏洞，在短时间内使用相同IP地址的用户会被当作是同一用户[7]；不管是被动或者主动的网络断线，再次连入时候都需要重新认证；Portal认证时，无论有效还是无效的终端都会获得一个IP地址，这对DHCP的资源消耗不少。另外，由于Portal是基于用户名和密码的认证模式，因此它只能满足对用户的管理，对于用户多个设备的管理却无能为力，无法继续细分[8]。

(3)MAC和Portal相结合的认证方式

通过对以上接入技术的分析，对于高校众多的无线用户来说，可以采用两者相结合的无感知方式进行认证。这种MAC和Portal无感知认证就是结合控制器和认证服务器给用户做一次二层(MAC认证)和三层(Portal认证)的认证[9]。用户连接WLAN不被要求用户名和密码，认证服务器自动获取终端MAC地址进行认证，整个过程不需要用户手动干预，全部是终端自动完成。这种无感知认证方式，将Portal认证方式的安全性与MAC认证方式的便捷性相结合，提高了用户体验[10]。

3 方案设计(Scheme design)

3.1 无线无感知认证需要解决的问题

针对以上提出的要求，要解决无线局域网无感知认证就要解决如下问题：

(1)要有统一身份认证的门户；

(2)终端设备第一次上线时需要进行认证，成功后终端MAC绑定用户，下一次上线直接无感知认证后接入网络；

(3)无线设备存在掉线、超时和移动漫游重连的问题，在发生这些问题后不需要重新认证。

3.2 统一认证的设计思路

学校目前采用的是基于LDAP协议(Lightweight Directory Access Protocol)的一卡通系统来存放用户数据。因此，只要无线系统支持LDAP协议就可以实现对用户的统一认证。

无线终端上线需要与AP关联，由DHCP服务器分配IP地址，然后无线控制器(AC)重定向，给用户推送相应页面，用户访问重定向的页面，即Portal服务器并获得认证页面，用户输入用户名和密码由Portal服务器将认证信息通过Portal协议发送给AC，AC将得到的认证信息发送给认证服务器RADIUS，认证成功后放行用户数据请求并把结果通知给Portal服务器，Portal服务器返回给用户认证结果，同时将终端MAC地址记录在数据库中，AC发送计费开始报文通知RADIUS服务器对认证用户进行计费。

无线控制器本身也提供MAC-Portal功能，在已知的MAC表中的终端设备被认为不需要手动进行用户名和密码认证，直接放行；未知的MAC地址会被重定向到Portal认证页面。但是，如果使用AC本地的MAC绑定和Portal功能来进行MAC地址匹配和Portal服务器，一方面支持用户的个数有限，另一方面会降低MAC认证的速率。

因此，为了实现大量用户的MAC地址快速认证，需要外置的Portal服务器来保存MAC绑定信息，并实现自动动态添加。

3.3 结合无缝漫游和无感知认证的设计思路

无线网络对用户终端的授权和认证是在无线控制器中实施的，这样即便无线终端发生漫游，只要终端的IP地址在移动的过程中不发生改变，用户的认证和计费信息也不会因为终端漫游而丢失。因此，DHCP服务器地址池和租约时间的配置以及DHCP服务器的网络结构，对于无缝漫游和无感知认证都具有重要的影响。具体可以通过以下方案解决：

(1)无线控制器提供DHCP服务，并且将所有无线用户的三层核心迁移到无线控制器上。

(2)合理规划DHCP地址池的范围和租约时间，既保证终端在一定时间内获取的IP地址保持不变，又要保证DHCP地址池地址充裕，以免后接入用户分不到IP地址。

(3)提供外置的Portal服务器，并串接到网络中，以达到准入的目的。

(4)合理划分无线用户VLAN，减少广播风暴的发生。

通过以上方案设计，用于认证的Portal服务器独立于为无线控制器，并且位于无线控制器的上层，用户进行漫游时，用户的认证和在线信息都保存在Portal服务器上了，再者用户设备在漫游期间IP地址不会改变，所以用户不需要再次认证。这样就做到了无缝漫游的无感知认证，如图1所示。

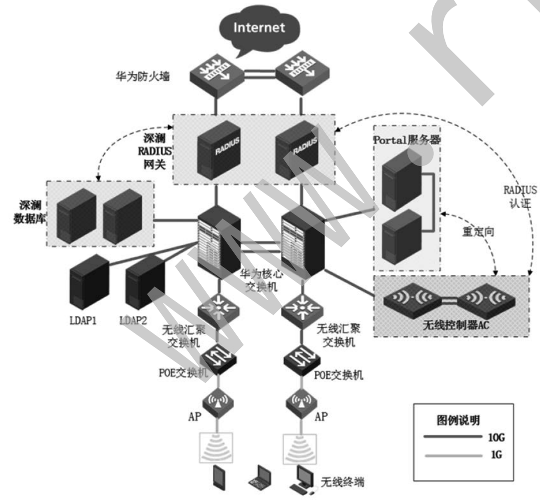

图1 无感知认证架构拓扑图

Fig.1 Topology diagram of non-perceptual authentication architecture

3.4 无感知认证流程

3.4.1 用户首次上线流程

无感知认证具备了“一次认证，终生有效”的优点。如果开通了MAC地址的快速认证，用户设备连入无线网络时，第一次登录Portal页面成功认证后，后续只要关联相应的该无线网络就可以直接放行，无须再填认证信息，如图2所示。

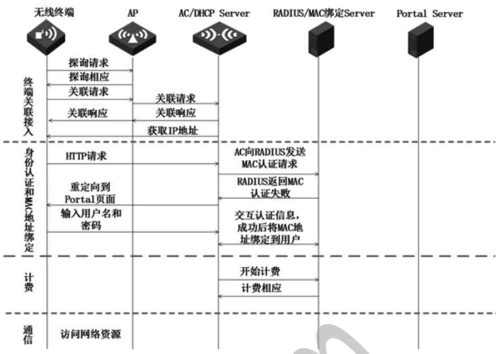

图2 用户首次上线流程

Fig.2 First access procedure for users

(1)用户启动无感知功能，终端设备通过AP连入无线网络。

(2)DHCP服务器分配所在AP对应范围(VLAN)的IP地址。

(3)用户请求访问网络，AP将HTTP请求发送到无线控制器AC。

(4)AC向认证服务器RADIUS发送MAC认证请求。

(5)RADIUS服务器根据AC所发的报文，验证MAC地址，并向AC返回认证失败结果(因为此终端设备第一次连入该无线网络，RADUIS服务器中没有绑定终端的MAC地址。)

(6)AC收到认证失败消息，根据Portal流程将重定向的认证页面推送给用户。

(7)用户提交用户名和密码信息完成Portal认证。

(8)用户认证成功后，在RADIUS服务器中将终端用户信息和MAC地址保存，同时，AC通知AP放行用户流量并且开始计费。

3.4.2 用户再次上线流程

用户设备再次上线时，只要终端MAC地址不发生变化，RADIUS服务器对设备流量直接放行，保持用户在线状态，此过程是终端设备和RADIUS服务器进行的后台交互，用户不参与该过程，从而达到无感知的效果，提升用户体验。流程图，如图3所示。

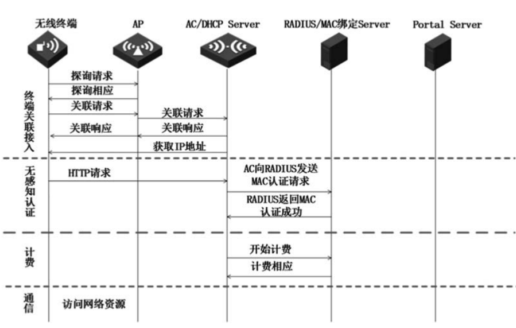

图3 用户再次上线流程

Fig.3 User reaccess procedure

(1)用户启用无感知认证功能，终端设备通过AP接入无线网络。

(2)DHCP分配相应IP地址给终端设备。

(3)AC接收到AP发来的用户HTTP请求，向RADIUS服务器发送MAC认证请求。

(4)RADIUS服务器根据AC发来的MAC信息，对比数据库中的结果(由于该设备已经完成过首次认证，用户的MAC地址、用户名/密码已经在服务器中存在)，向AC返回认证成功消息。

(5)用户认证成功，正常上网并计费。

4 方案实现(Scheme implementation)

前面已经对用户终端设备的无感知认证方案进行了探讨和分析，接下来将在北京石油化工学院校园WLAN环境中实现上述方案。

4.1 无线网络环境

北京石油化工学院无线局域网覆盖了全校各个区域，包括办公、教室、宿舍、室外等，总计2600多个AP和两台堆叠方式的AC，均使用的是H3C的不同型号产品。采用深澜软件系统，其中包括两台串接在出口的网关，两台开启Portal、RADIUS以及MAC绑定功能的服务器，两台深澜数据库服务器，其中RADIUS的认证功能连接到校内LDAP认证系统，实现有线、无线统一认证。H3C无线控制器AC的型号为WA5540H。

4.2 设备配置过程

4.2.1 无线控制器的配置方案

AC在整个无感知应用环境中起主导作用，主要实现了AP的管理、DHCP服务器、用户VLAN的三层地址、对终端的认证和授权以及与深澜系统的对接等功能。

(1)在AC提供DHCP 服务，配置相应的DHCP参数。

```
dhcp server ip-pool vlan102
gateway-list 10.10.104.2
network 10.10.104.0 mask 255.255.252.0
dns-list IP1 IP2
expired day 0 hour 4
```

其中DHCP地址池要保证该区域每用户能得到三个IP地址，租约时间较为重要，起初设置的是12小时，因为采用了无感知方案，用户终端只要在无线区域内就可以连入接入网络，导致IP地址被无意中占用很多，部分区域DHCP池一度枯竭。后来经过不断调整，DHCP池的占用率峰值在75%左右，达到合理范围。

(2)将用户的三层核心移到AC中，确保无缝漫游。

```
interface Vlan-interface102
ip address 10.10.104.1 255.255.252.0
portal nas-port-type wireless
```

(3)按照区域规划用户VLAN，保证每区域IP范围不超过四个C类地址。

```
interface Vlan-interface102
ip address 10.10.104.1 255.255.252.0
portal nas-port-type wireless
```

(4)配置AP的统一模块，确保所有的AP都在同一个SSID下面，确保终端移动过程中的无缝漫游。同时，确定MAC认证和Portal服务器的应用模版。

```
wlan service-template 20
ssid bipt
client forwarding-location ap vlan 102 to 120
client forwarding-location ap vlan 203 to 208
client-security authentication-mode mac
client-security ignore-Authentication
mac-authentication domain mac-shenlan
portal enable method direct
portal bas-ip IP-AC
portal apply web-server portal-shenlan
portal nas-port-type wireless
service-template enable
```

(5)配置用户的被动下线策略和AAA认证。

```
domain mac-shenlan
authorization-attribute idle-cut 20 100000
authentication lan-access radius-scheme bipt-shenlan
authorization lan-access radius-scheme bipt-shenlan
accounting lan-access radius-scheme bipt-shenlan
```

在该方案中，AC负责监控用户数据流量，在一定时间内(比如20分钟)流量小于100kB，AC就会向AAA发送计费结束报文，同时强制用户下线。这种方式称之为idle-cut方式。

(6)在AC中指定Portal和RADIUS服务器的地址和通信密钥。

```
radius dynamic-author server
client ip IP-Portal key cipher paasword
portal web-server portal-shenlan
url http://IP-Portal/index_4.html
server-type cmcc
portal server portal-shenlan
```

ip IP-Portal key cipher password

port 2000

portal mac-trigger-server mts-shenlan

ip IP-Portal

4.2.2 深澜计费认证体统的配置方案

由于无感知认证的发起者是无线控器AC，大部分的配置都在AC上，相对于RADIUS(AAA)来说，主要完成以下配置：

(1)和学校现有的LDAP做对接实现统一认证：

LDAP服务器地址：IP地址

LDAP服务器端口：389

Root DN:cn=Manager,dc=bipt,dc=edu,dc=cn

Root密码:PASSWORD

User DN:ou=People,dc=bipt,dc=edu,dc=cn

(2)在深澜系统中的控制策略中开启MAC认证(无感知认证)和MAC地址绑定，并且可是设置自动收集MAC地址的数量，本方案中设定值为5。

(3)用户可以在自服务中手动添加、删除已绑定到自己一卡通帐号下的MAC地址，并且可以根据自己所需是否开启无感知功能。

(4)为保证无感知认证用户的安全性，限定同一帐号下最多同时有三个在线，下个设备上线是提示“超过”最大连接数量。

4.3 方案验证

主要验证两个功能，一个是无感知认证过程，另一个是终端漫游。

(1)终端设备第一次接入WLAN时会弹出认证Portal页面，输入一卡通的用户名和密码后，直接连入互联网并开始计费。主动断开或者被踢下线后，再次接入WLAN，无须任何操作就可以直接上网，经查询，MAC绑定服务器中已经存在该用户信息和MAC地址的绑定关系，删除该信息后，用户接入WLAN时需要再次经过Portal认证。

(2)用户终端从AP1移动到AP2的过程中，由于一个终端同一时刻只能连入一个AP，终端会自动协商而短暂中断，断开时间不超过2秒，有的区域甚至是毫秒级，仅丢失一个数据包，这取决于无线网络的覆盖范围，都是在允许的可接受范围之内。无缝漫游功能实现。

经过部署，北京石油化工学院的WLAN认证系统以MAC-Portal作为准入认证手段，同时协同多种技术共同构建的无感知认证技术方案经过测试和用户反馈，证明整体设计方案及实施过程是可行的，并且易于扩展，网络设备的架构均采用的是冗余热备或并行方式，避免了单点故障所引起的网络和认证中断。同时，无线控制器提供了完整的日志查询，能够清晰定位用户信息和用户的网络使用情况，这对于未来其他系统如考勤、定位用户轨迹、为用户推送相应页面都提供了较为完整的数据基础。

5 结论(Conclusion)

校园无线网的准入方案对于校园网安全来说至关重要，本文将校园网安全性与用户易用性相结合，设计实现了一套可用于任意规模园区的通用无线无感知认证方案。该方案对于用户来说，简化了用户的接入无线网络流程，极大地提高了用户的易操作性和体验感。同时，对于校园网安全来说，不仅做到了授权准入，精准控制，而且还提供了完备的日志查询和信息追踪，很好地保障了校园网络信息化安全。

参考文献(References)

[1] Debiao HE,Ding WANG,Qi XIE.Anonymous handover authentication protocol for mobile wireless networks with conditional privacy preservation[J].SCIENCE CHINA,2017,5(60):1-17.

[2] Yu HUANG,Liang JIN,Hongquan WEI.Fast Secret Key Generation Based on Dynamic Private[J].NETWORKS & SECURITY,2018,11:171-183.

[3] Ye LIU,Fulong JIANG,Hao LIU.Interference Robust Channel Hopping Strategies for Wireless Sensor Networks[J].China Communications,2016,3:96-104.

[4] 蔡云鹏,刘哲,蔡娇.基于无缝漫游的WLAN无感知认证研究[J].计算机科学,2017,10A(44):202-206.

[5] 冯雷,林初建,赵君.MAC与Portal相结合的无感知认证技术研究[J].华中师范大学学报(自然科学版),2017,5:4-8.

[6] 李刚,刘威,王洪信.Portal结合DHCP的校园无线网络无感知接入技术研究[J].计算机科学,2017,10A(44):305-307.

[7] 王道佳,马严,黄小红.基于DHCP的校园网准入及无感知方案研究[J].华中科技大学学报(自然科学版),2016,10(44):181-185.

[8] 邱知文,张杰.基于校园无线网的BYOD认证系统设计与实现[J].计算机应用与软件,2015,2(32):94-96;147.

[9] 杨璐.校园WLAN无感知认证方式分析[J].信息安全与技术,2015,1:22-24.

[10] 胡建龙,王莎莎,王宇翔.基于无感知的校园无线网络认证策略研究[J].计算机科学,2015,11(b):120-121.

作者简介：

王　玮(1978-)，男，硕士，网络高级工程师.研究领域：计算机网络及其应用.