The Experimental Campus WLAN Roaming System and WiMAX Integration in Taiwan

Wei-Hung Huang [1], Ko-Chung Tang [1], Zsehong Tsai [2]
[1]Network Technology Division, National Center for High-Performance Computing, Taiwan
(allen_huang@nchc.org.tw, Kevin@nchc.org.tw)
[2] Graduate Institute of Comm. Engineering, National Taiwan University, Taiwan
(ztsai@cc.ee.ntu.edu.tw)

***Abstract*— WLAN have emerged as a promising network platform and extended network connectivity in recent years. Hotspots are increasing rapidly in coffee shops, airports, restaurants and some public areas. In Taiwan, over 90% of colleges and universities have established their campus WLAN environment and 72% of them have joined the experimental campus WLAN roaming system. This paper describes how we have established such a WLAN roaming system. Relying on the RADIUS based authentication environment, a campus WLAN user can enjoy WLAN roaming service via web portal or 802.1x based AAA system. Newly developed applications such as voice/video service can be tested on this system. This paper will also introduce how this system integrated with WiMAX and deliver the inter-working capability.**

Keywords: **AAA, Roaming, WLAN, WiMAX**.

I. INTRODUCTION

Due to the promotion of the M-Taiwan program by Taiwan government, establishing a wireless environment has become increasingly popular for Taiwan's universities, colleges and other public areas such as coffee shops, libraries, airports, and hotels. The establishment of IEEE 802.11 based WLAN environments on the campuses of Taiwan's colleges and universities has thus become an important sector of their campus network for the past several years. Although campuses generally utilize the standard IEEE 802.11 a/b/g WLAN, they still establish their own independent WLAN AAA environments. As a result, every campus' WLAN environment is like an isolated island that can only be used by their students, teachers and work force. Such an island-like campus WLAN environment directly contradicted one goal of the M-Taiwan project which aimed to create an island-wide broadband wireless environment, and implies that no two universities or colleges can enjoy the benefit of wireless resource sharing.

Since the development of campus WLAN resource sharing and integration has been a hot topic around colleges and universities, the experimental campus WLAN roaming system was initiated to integrate campus WLAN resources in Taiwan's campus community, on a volunteering basis. This large scale integration requires the WLAN authentication mechanism in all participating campuses to use the same or interoperable authentication platform to access WLAN services, so that any campus user can be authenticated in a visiting campus. In the following, we will describe how such platform is developed. In addition, the WiMAX has become an important emerging wireless technology to be employed in the city and campus, we also described how this campus WLAN roaming system can be integrated with WiMAX service.

II. THE ARCHITECTURE AND AUTHENTICATION MECHANISM OF THE CAMPUS WLAN ROAMING SYSTEM

The campus WLAN roaming system was started to be sponsored by the National Science Council (NSC) and instructed by the National Science and Technology Program for Telecommunications (NTP). The goal of this roaming system is to establish a campus WLAN roaming mechanism and architecture, to provide service and technical consultation for the system, to integrate WLAN resources of all campus, to develop new applications, and to jump start the development of new wireless industries within Taiwan.

There are total of 163 colleges and universities in Taiwan. 90% of them have established campus WLAN environment and 72% of them have joined this experimental campus WLAN roaming system. By December, 2007, the number of campuses and research institutes which joined this system had reached 118[1]. All the 118 campus and research institutions can share the WLAN resource to one another.

The campus WLAN roaming system is comprised of the participating campus' WLAN equipments including their Access Point, Access Control Gateway, Authentication Server, Roaming Server, and Roaming Center. The architecture is illustrated in figure 1.

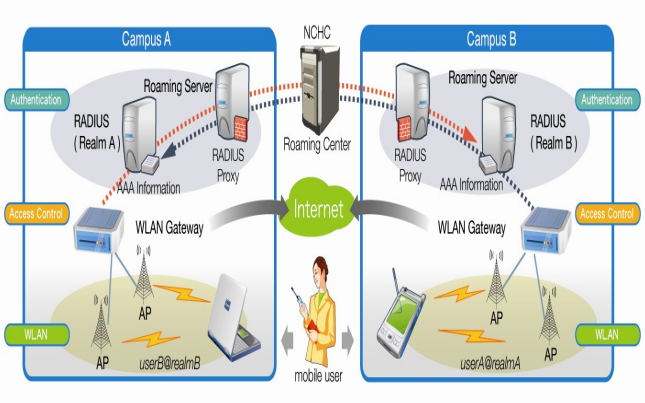

Figure 1. The architecture of campus WLAN roaming system

The WLAN roaming authentication system is based on Remote Access Dial in User Service (RADIUS)[2][3] which is integrated into each campus' user account database. When the user is on visited campus and trying

to access the WLAN, the WLAN gateway will authenticate the user and pass the authentication message to local Roaming Server. The local Roaming Server will pass user's identity to the Roaming Center, which will, in turn, pass the identity back to his home campus to perform the authentication process.

The Roaming Center supports many authentication protocols including PAP/CHAP, EAP-MD5, EAP-TLS, EAP-TTLS and EAP-PEAP and connects with the participating campus' Roaming Servers via virtual private network (VPN)[4]. Also, it has all of its networked institutions' related information and is responsible for authentication message switching. It is the core of the roaming authentication system. The VPN tunnels between Roaming Servers and the Roaming Center are used for protecting authentication message when they are using the roaming system. The software architecture of the roaming center is illustrated in figure 2. Using the roaming authentication system, campus members can share other participating campuses' resources. Thus, the goal of campus WLAN resource integration has achieved.

Currently, there are two main campus WLAN authentication mechanisms in Taiwan. They are web portal and 802.1x. Some campuses' WLAN infrastructure was established long ago, there did not support 802.1x EAP authentication mechanism. Therefore, we need a WLAN access gateway to control the users' access to the campus WLAN. Whenever a user use NB or PDA to access the WLAN, the user will be asked to authenticate by entering his account and password. Once the user has passed the authentication process, he will be able to go online.

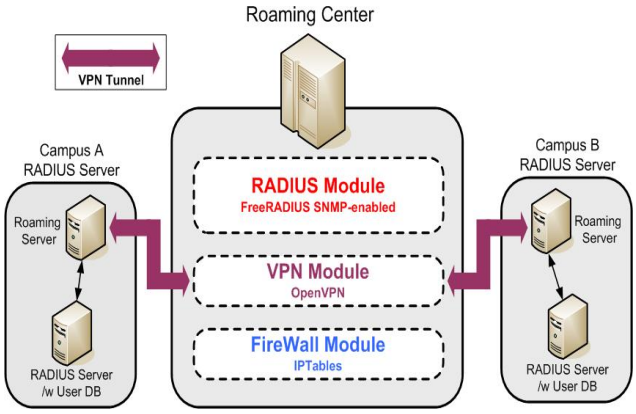

Figure 2. Software architecture of the Roaming Center

Web portal uses Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) as its authentication protocol. The process is as follow:

1) When user turn wireless equipment on and sets the Service Set Identifier (SSID) correctly, user will connect to the WLAN.
2) User automatically receives an IP address from the Dynamic Host Configuration Protocol (DHCP).
3) When user opens his web browser, the WLAN access gateway will redirect user to the authentication webpage.
4) The user then must enter account and password which are then passed through the WLAN access gateway to the RADIUS server for PAP/CHAP authentication. Only if the authentication process succeeds, the WLAN access gateway will open a session for the user to get online.

802.1x[5][6] is another choice for the wireless authentication mechanism. The 802.1x standard defines how to authorize the users' access to Ethernet network by managing the virtual ports. Currently, the 802.1x standard is the most widely used in the wireless industry. If the user passes the 802.1x authentication process successfully, the WLAN access point or gateway opens a virtual port for him to go online. However, if the process fails, no virtual port will be opened and no further communication can take place. The 802.1x authentication mechanism has three fundamental parts:

1) Supplicant: a wireless user.
2) Authenticator: a wireless access point which won't allow a user to access the network until he passes the authentication process.
3) Authentication Server: the RADIUS server which authenticates a user's information and then responds to the Authenticator.

The supplicant and the authenticator use the Extensible Authentication Protocol (EAP) to transfer information to each other and then to decide the EAP communication type.

In this campus roaming system, most of the participating campus use web portal as their authentication mechanism. Very few use 802.1x. Web portal and 802.1x have different authentication processes and account information formats. Not every campus' WLAN access equipment can support both web portal and 802.1x, campus which uses different authentication mechanisms may not exchange users' identity information successfully. For this reason, campus should deploy or upgrade their WLAN access equipment for supporting both web portal and 802.1x. Even though most of the participating campus use web portal as their authentication mechanism, it does have several security issues. Because of this, we will promote 802.1x as the primary authentication mechanism and help campus upgrade their equipment and authentication server to support 802.1x.

III. Campus WLAN Roaming Security Enhancement

Wireless network environments are less secure than ever before due to the increasing sophistication of the hacker's tools. More and more campus and research institutions join this WLAN roaming system. There are almost over six hundred thousand user accounts on this system. We are trying to discover a low-cost solution to strengthen the security of campus WLAN roaming system, and the following is the security mechanism that has been promoted in campus WLAN roaming system.

A. Enhancement of web-portal Authentication Environments

In Taiwan, most of the campus wireless networks use web portal as their authentication mechanism. Only 5%

of the campus wireless networks use the 802.1x EAP-TTLS or EAP-PEAP mechanism. In most situations, users complete the authentication process using their web browsers. This could be dangerous. Web portal authentication mechanisms are popular because they are easy to establish and use. They have many security issues though such as rogue AP, malicious authentication websites, fake authentication servers, etc.

One goal of this roaming mechanism is to strengthen the wireless network environment security by using the experimental WLAN roaming Certificate Authority[7]. The experimental WLAN roaming CA is responsible for signing and distributing digital certificates to the participants' wireless authentication equipment. These certificates can be used as the foundation of the websites' Security Socket Layer (SSL) encryption and provide users an easy way to identify the authentication web-portal. These certificates also are needed if we want to use the Protected Extensible Authentication Protocol (PEAP)[8] or the Tunneled Transport Layer Security (TTLS)[9] as the authentication mechanism under the 802.1x authentication environment. Furthermore, the administrator can manage the WLAN roaming environment more efficiently and safely.

B. 802.1x EAP-PEAP/TTLS based Authentication Mechanism with Early Tunnel Termination

EAP-PEAP and EAP-TTLS are two promising 802.1x authentication protocols that have been used on the campuses of Taiwan's colleges and universities. EAP-PEAP/TTLS has the anonymous outer-identity function which hides the user's personal information. The anonymous function is shown in figure 3.

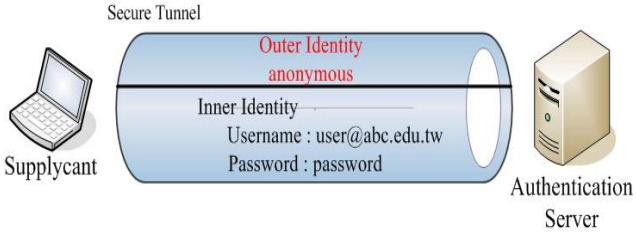

Figure 3. Outer/Inner Identity in PEAP/TTLS message

The outer-identity is responsible for building the secure tunnel to home authentication server. The inner-identity is the real user credential which is inside the outer-identity. When in roaming, if user gives anonymous or wrong information in outer-identity, the secure tunnel will be fail or connecting to wrong place. It may cause the error in authentication or accounting record. When using EAP-PEAP/TTLS WLAN roaming authentication mechanism, it would be better to use the Early Tunnel Termination and establishing the RADIUS accounting mechanism at the same time to prevent management difficulties when user use the Outer Identity anonymous function. Figure 4 illustrates the EAP-PEAP/TTLS with Early Tunnel Termination. By doing so, the management of the campus WLAN authentication and accounting will be more easy and correct.

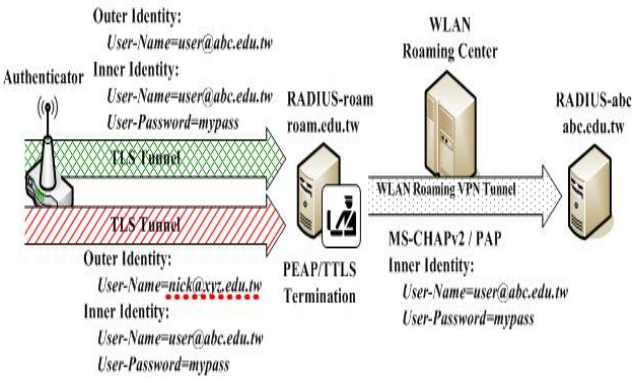

Figure 4. EAP-PEAP/TTLS Authentication with Early Tunnel Termination

IV. THE SERVICE INTEGRATION OF CAMPUS WLAN SERVICE AND WIMAX

In addition to the WLAN, there is another promising technology called the WiMAX, emerging in the campus network. The IEEE 802.16d/e standards[10][11] (as know as WiMAX) is for high-speed wireless MAN connectivity and have larger covered regions, therefore, it is able to provide users with a high degree of usability. Currently, some universities and collages begin to deploy the fixed or mobile WiMAX environment for test and research purpose. The telecom operator or WISP also deploy and will provide WiMAX service soon. Therefore, it would be convenient to use the WiMAX networks on campus. This section will describe how the experimental campus WLAN roaming system integrated with the WiMAX service.

A. The Authentication Mechanism integration of Campus WLAN Roaming System and WiMAX

If we want to integrate the WLAN and WiMAX services, a good user authentication mechanism must be developed. The EAP authentication mechanism is suitable for WiFi and WiMAX environment. EAP-TTLS is one of recommended authentication methods by the WiMAX Forum[12], and EAP-TTLS can support vary kind of user account/password databases , just like UNIX shadow/passwd, LDAP etc. Many types of authentication algorithms may be used inside the encrypted tunnel., i.e. MS-CHAPv2, MS-CHAP, CHAP, PAP, EAP and others. EAP-TTLS is not similar to EAP-PEAP, it does not care about what kind of password type is stored in the database. EAP-PEAP can only support the clear-text type of password format which 95% of colleges and universities do not support in Taiwan. From this point of view, EAP-TTLS is recommended to be a best choice for migrating the service from WiFi only to a WiFi-WiMAX coexisting environment while allowing all current campus WLAN users to continuing enjoy campus WLAN roaming service and using the same single account. WLAN administrators need only to upgrade or integrate WiFi and WiMAX with fewer efforts. The architecture is illustrated in figure 5.

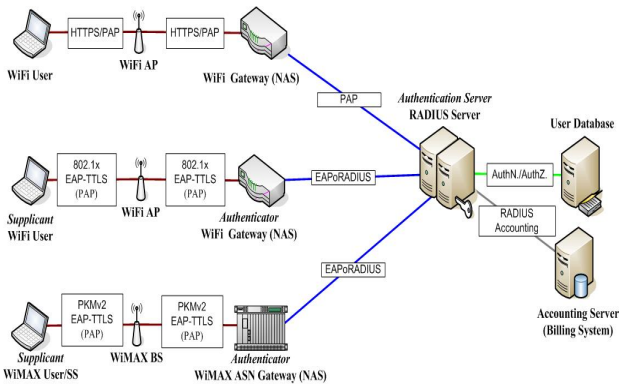

Figure 5. EAP-TTLS authentication mechanism in the WiFi/WiMAX coexisting environment

B. *The interworking between Campus WLAN Roaming Service and WiMAX service*

According to the mobile WiMAX development situation in Taiwan, six WiMAX licenses has already been released by National Communications Commission(NCC) in Taiwan. By regulation, the operators must provide the WiMAX service within three years. Some operators probably provide trial service and test within one year. Some campuses may enjoy the WiMAX service soon. This experimental system cooperated with the WiMAX operators in Taiwan and has tested the following two scenarios of integration of WiMAX and Campus WLAN Roaming service with PKMv2[13] EAP-TTLS authentication mechanism.

1) *The architecture of campus operator mode*

The so-called campus operator mode means that the campus is similar to WLAN operator. This mode allows the mutually benefits or commercial roaming between the campus and WiMAX operator. Under this architecture, the campus user can use the WLAN inside campus with WiFi device. If the campus user have WiMAX-enable device, they can use the operator's WiMAX service by passing the authentication information back to campus's AAA server. The architecture of campus operator mode is illustrated in figure 6.

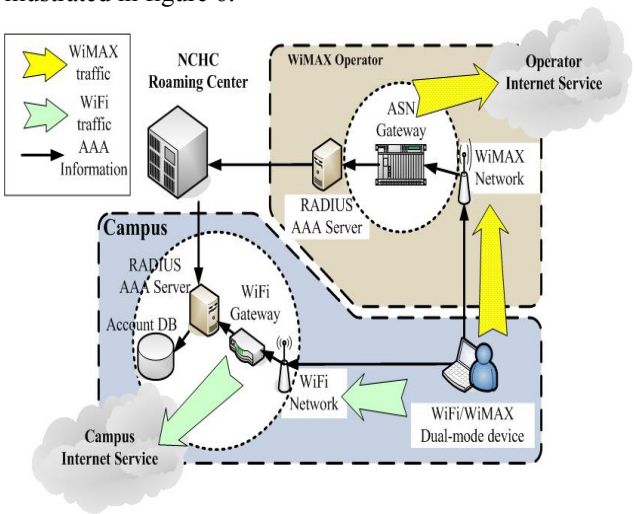

Figure 6. The architecture of Campus Operator mode

In this architecture, it will be the most efficient way to exchange user AAA information through the Campus WLAN Roaming Center. The AAA server of WiMAX operator must recognize the account format from campus user, and pass the authentication request to AAA server in campus. The campus user can use the WiMAX operator's internet service after they had been authenticated by campus AAA server, and do not need another WiMAX credential. In another word, the campus user can use campus WLAN roaming service and operator's WiMAX service with signal account. In the concrete, the subscriber of WiMAX operator also can use campus WLAN service with they own credential when they in campus. Because of some operators provide EAP-AKA authentication, the subscriber can use SIM card as they identity when using the WLAN service in campus.

2) *An alternative model to campus ADSL service*

The second architecture is the alternative to campus ADSL service. In Taiwan, some universities and colleges provide the ADSL service to work force, teachers and students. They can connect back to campus' network and use internet service via campus ADSL. In this architecture, the operator offer partial WiMAX service and connect to campus network backbone via VPN/VLAN. The campus user uses the WiMAX service to replace the ADSL service. The universities and colleges do not need to maintain the ADSL equipment any longer, but may cooperate with WiMAX operator. The campus user still can use the original campus WLAN service, and also can use WiMAX service outside campus. Figure 7 shows the campus ADSL alternative mode.

This scenario is similar to campus user using ADSL to connect back to campus network backbone. It is popular with campus and user because the user can take the ADSL to go, and not been limited in fixed place. In this architecture, the internet traffic of campus user will not pass through the operator's backbone. The traffic will route to campus network via VPN/VLAN. If the WiMAX signal can cover the whole campus area, it can mend to deficiency of the campus' WiFi coverage and the campus' user also can use WiMAX service inside campus. The subscriber of WiMAX operator cannot use campus WLAN service in this scenario.

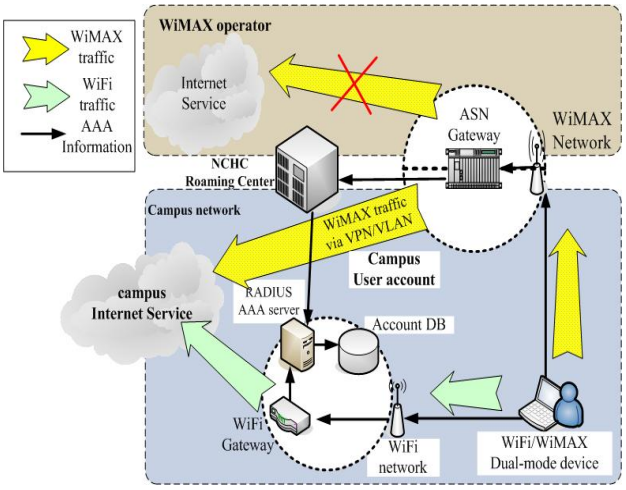

Figure 7. The architecture of alternative model to campus ADSL service

V. CONCLUSIONS

This experimental system has now been successfully developed in Taiwan and would be a great asset to the future development of potential wireless applications. For example, this environment is ready for the testing of a campus VoIP services. As long as the WiFi/WiMAX handset is ready then campus network can be used as their test bed. Since one major goal of this system is to combine each campus' WLAN environment so that campus activities such as off-campus teaching, sightseeing, and digital browsing can be further developed, we believe further integration of VoIP/IP video services over this roaming mechanism is highly desired. Further more, some specific applications which provide by operators also can be developed and tested over this test-bed, such as intelligent transportation systems, location based service, novel entertainment system etc.

WiMAX extends the connectivity of WiFi to deliver the next-generation mobile internet service. The integration of WiFi and WiMAX deliver the convenient and broadband internet service that brings new development model for operators and campuses. At the beginning of 2008, the U-Taiwan project was initiated. One goal of the U-Taiwan project is that user can access the internet anytime, anywhere. Along with the U-Taiwan, this roaming system will continue to develop and promote the island-wide wireless access environment. It is expected to create many new opportunities for wireless network development, stimulate the development of related industries, and increase international cooperation.

REFERENCES

[1] Campus WLAN roaming environment web site, http:// wlan rc.nchc.org.tw

[2] RFC2865 - Remote Authentication Dial In User Service (RADIUS), Jun 2000.

[3] FreeRADIUS, http://www.freeradius.org

[4] OpenVPN, http://openvpn.sourceforge.net

[5] RFC 2284 - PPP Extensible Authentication Protocol (EAP), March 1998

[6] RFC 3579 - RADIUS Support For Extensible Authentication Protocol, Sep 2003

[7] Campus WLAN roaming environment CA web site https:// wlanrc.nchc.org.tw/CA

[8] EAP-PEAP (Internet draft), http://www.ietf.org/internet-drafts/draft-jose fsson-pppext-eap-tls-eap-08.txt

[9] EAP-TTLS (Internet draft), http://www.ietf.org/internet-drafts/draft-ietf-pppext-eap-ttls-05.txt

[10] IEEE, "802.16-2004", http://standards. ieee.org/ getieee802/ download/ 802.16-2004.pdf

[11] IEEE, "802.16e-2005", http://standards .ieee.org/ getieee802 /download/ 802.16e-2005.pdf

[12] WiMAX Forum, "WiMAX End-to-End Network Systems Architecture Stage2-3 Release 1.0.0", http://www.wimaxforum.org/technology/docu ments/WiMAXNetworkArchitectureStage2-3Rel1.0.0.zip

[13] Adibi, S.; Bin Lin; Pin-Han Ho; Agnew, G.B.; Erfani, S.," Authentication Authorization and Accounting (AAA) Schemes in WiMAX" IEEE Internationa lConference on Electrol information Technology, pp. 210-215 , May 2006