Construction of Junior High Schools and Elementary Schools Wireless LAN Authentication and Encryption Management Mechanism in Taoyuan County

Shih-Kai Chuang *
Department of Electrical Engineering, Yuan Ze University
s944728@mail.yzu.edu.tw

Chin-Ping Chuang
Department of Computer Science and Information Engineering, National Taiwan Normal University
u91043@csie.ntnu.edu.tw

Hao-Cheng Yang
Department of E-Learning, National Chiao Tung University
cccp.nl95g@nctu.edu.tw

Ming-Yi Chen
Department of Information Management, Kainan University
m94221004@ms2.knu.edu.tw

Ming-Wen Chang
Director-general, Bureau of Education Taoyuan County Government
cmwtnu@ms.tyc.edu.tw

Abstract

With the rapid development of Internet, network infrastructure is becoming increasingly complex. After building up a complete wireless network environment and related equipments, wireless network security management turns into an important issue. Because of a lack of funds for maintaining IT equipments and most of the primary school teachers don't have adequate network management capabilities, we design a Wireless authentication management mechanism for all elementary and junior high schools in Taoyaun. All staffs in this program can use their educational learning center passport account and password to surf the Internet and we can do concentrated possession at the same time.

After a year of online testing, modification and performance analysis, we confirmed that this mechanism can effectively manage school wireless Internet access, reduce network abuse and virus attacks and provide better quality of wireless Internet access.

Keywords: WLAN, SSLVPN, ACLs, Security

1. Introduction

With the continuing development of Internet – going from wired to wireless, network infrastructure is becoming increasingly complex and the number of Internet users is also growing rapidly. In the campus, apart from the use of wired networks, wireless Internet use is also raising. How to enable schools to manage wireless networks effectively becomes another important issue. However, the campus human resources and facilities are limited. Managers not only need to provide quality basic services, avoid wastage of network resources for using network facilities properly, but also to build an omni-directional network engineering and operation management system in order to manage more than 200 school's wireless network systems in Taoyuan county, which can allow managers to maintain and manage this authentication and encryption system in an easiest way.

In junior high and elementary schools, the number of staff using Internet is numerous. It is quite common that IP supply is unable to meet the demand with current IPv4 technology.

Therefore, for more effective management, appropriate allocation of resources, and wireless data transmission encryption, a good network of management systems are necessary, such as: authentication and encryption system, etc. [9].

In campus wireless network management, which was controlled by county/city centers and universities, most of them allocate an authentication server (such as: RADIUS) for the account and password authentication. In order to avoid repeated use of account, we always increase the record of MAC for controlling ACL. Because of the use of information, the system must be set up with the same network segment as Gateway. However, the costs of purchasing certification system or building up certification server at junior high and elementary schools are too high and the certification roaming system architectures are too complicated as well. Because of the limited human resource at junior high and elementary schools, the use of this structure (Figure 1.) will increase management and network troubleshooting difficulties.

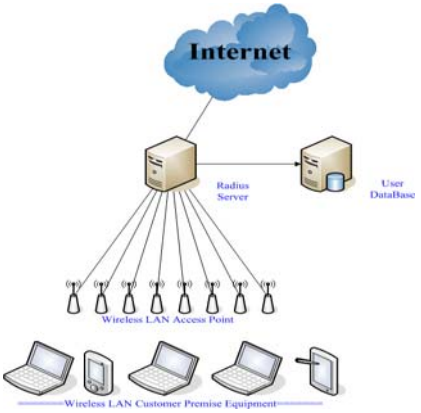

Figure 1

A general wireless network authentication

We proposed new network authentication and encryption architecture, all users, whether wired or wireless network users, can establish

VPN connection after certification through encryption Web-based authentication system to replace the traditional authentication methods and introduce SSLVPN technology without exception.

School staff uses their account password to log-in, even outsiders can also use the Internet Guest account, but they are restricted to use the Web Service. There is no need to take care of authentication mechanism management in centralized authentication architecture for the end of the network management center staff, so it's much easier to maintain and to effectively prevent network abuse. Furthermore, we can use VPN technologies to set up encryption connection from users to server and provide new Public IP from server. From this mechanism, we can separate wireless network from internal LAN network and avoid external visitors to introduce network viruses. Relevant information will be recorded, and it can be used via some data mining technologies for extracting user Internet behavior in the future.

2. Existing Network Authentication System with Wireless Encryption Security Mechanism

2.1 POP3 authentication connection mechanism

For users who already set up e-mail servers, it can be cascaded with user database which was built by wireless equipment using POP3 identity verification mechanism. It can verify only user name and password, but as long as the database servers and wireless equipment start the POP3 protocol, this mechanism can be integrated with other authentications. It is a very simple method and does not need any complicated settings. But it's not suitable for the departments which need higher security requirement [10].

2.2 RADIUS/LDAP

In order to ensure the safety of Identity verification, it might be the best way to use RADIUS and LDAP. User database integrate front-end wireless devices via RADIUS/LDAP. When users connect to Internet, wireless base station asks for the back-end database to confirm the identity information of users and to provide corresponding wireless network services. Such approach is suitable for large-scale use of wireless environment and RADIUS/LDAP server can support multiple backup. As long as the wireless devices can simultaneously support multiple RADIUS/LDAP servers, it can ensure the high availability [10].

2.3 IEEE 802.1x

IEEE802.1x is an approach which uses Radius servers to authenticate user identity with user's computer using CA certificate. Wireless base station is only responsible for sending signals, and is not responsible for handling network authentication, as illustrated in figure 2.

CA certificate must be installed in the wireless client-end computer, so it might increase the loading of user, on the contrary. Therefore, the equipment manufacturers have developed a simpler 802.1x certification mode to install the CA certificate at wireless network equipment server-end. User can connect to login page through HTTPS link, and wireless-network equipment can be wireless base stations, routers or switches, can also be seen as proxy servers. Back-end user database still takes charge of the processing of user identity authentication. Front-end computer does not need to install CA certificate. It can reduce the work burden on the network [10], but this kind of equipment is expensive in general.

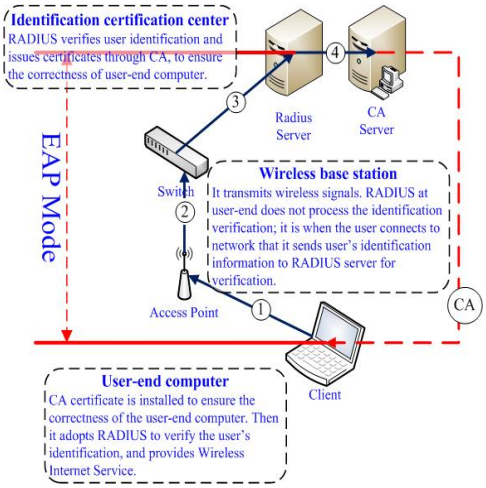

Figure 2

IEEE 802.1x authentication framework

IEEE802.1x is a security method based on EAP (Extensible Authentication Protocol) which is a communication protocol framework, not just a communications protocol or user identification identity, but also can be used for designing their own network environment. At 1990s, 802.1x has been defined in IETF RFC3748. It was first applied to the wired network PPP dial-up, and later extended to the wireless network field, as illustrated in figure 3 [10].

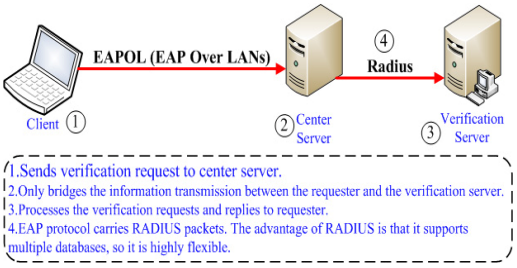

Figure 3

IEEE 802.1x authentication flow chart [10]

2.4 WEP Encryption

WEP (Wired Equivalent Privacy) is one of encryption method defined in 802.11. We can set a key on the wireless base station (A station can be set four keys at most). The wireless base station would have the key coding encryption, and only the users who enter the same keys can allow establishing the connection.

In WEP, it adopts RC4 algorithm in encryption algorithm field. The key length must be 40 bits. It also applies another mechanism to combine a 24 bits initialization vector (IV) and the WEP key as 64 bits or 128 bits key.

The wireless network base station provides four modes to generate the key: The first mode, users enter hexadecimal numbers directly; the second mode and the forth mode are similar, where users enter a string and encrypt automatically to generate hexadecimal numbers. In these 3 modes, users need to enter 13 hexadecimal numbers to establish connection. In the third mode, users only need to enter characters (alphabetical letters) that we usually use and this mechanism can generate hexadecimal numbers, as figure 4 [8].

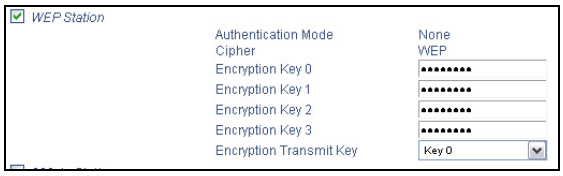

Figure 4

Select 128bit encryption and enter the key via Passphrase method

2.5 WPA Advanced Encryption

Although WEP provides the basic security protection of wireless network, it is still too fragile. As the method, which cracks RC4 keys, went published by Fluhrer in 2001, an open source program for cracking WEP program was spread on the Internet, even the 128 bits encryption code length can be resolved in a short period of time.

Therefore, IEEE defined a more restrained standard 802.11i. Because this standard had not been passed yet and in order to let manufacturers having a basis for reference first, in 2002, Wi-Fi Union made a 802.11i draft to a tentative standard which is called WPA (Wi-Fi Protected Access).

WPA = TKIP + MIC + 802.1x + EAP

In this WPA equation, 802.1x and EAP are authentication mechanisms; TKIP and MIC are stronger encryption mechanisms. Wi-Fi Union wishes that they can provide a more secure wireless network connection. Most of wireless high quality base stations will provide WPA [8].

Figure 5

The WPA method which provides higher security is similar to WEP method, but has different contents in code

2.6 Summary

There are difficulties in using, setting and managing these security encryption methods in elementary and junior high school campus. We compare and analyze these methods as in Table 1.

In view of this conclusion, we don't use WEP or WPA encryption mechanism which needs the supports of network base station and operating system. We propose a new integrated network authentication and encryption system attaching with SSLVPN mechanism and Radius authentication scheme to alleviate the pressure of managers in these elementary and junior high schools. We will explain the related techniques and operational theorems in next chapter.

Compared Item		Security	Establish Difficulty	Use Difficulty	Cost
WEP		Low	Easy	Difficult	Low
WPA		Medium	Medium	Difficult	Low
VPN	PPTP L2TP IPsec	High	Difficult	Difficult	Medium
	VPN Client	High	Medium	Difficult	High
	SSLVPN	High	Easy	Easy	Medium

Table 1

Comparison of various security encryption technologies

3. System Operational Theorem and Architecture

When wireless network users link to the wireless base station, they can open the web browser and connect to any website. The server will link to our SSLVPN authentication system automatically. After finishing the certification, the system will establish VPN network to ensure the security of wireless transmission and connect to Internet.

3.1 Center-end Architecture

At center-side, we install SSLVPN network authentication system and set up Radius server to access accounts/passwords data in our county research and study database, as illustrated in Figure 6 and 7. Then we use FreeRADIUS to access PostgreSQL database. However, the table

data definitions between original database and FreeRADIUS are different. So, we need to use PostgreSQL view to construct FreeRADIUS format data sheet at first, as illustrated in figure 8 and 9.

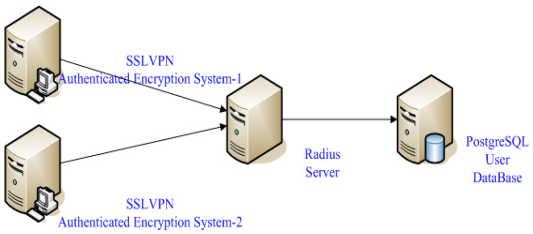

Figure 6

Account authentication system architecture

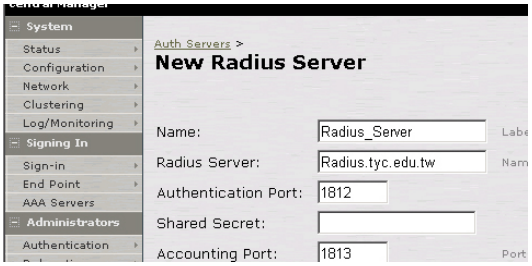

Figure 7

SSLVPN certification connection settings

```
# The default queries are case insensitive. (for compatibility with
# older versions of FreeRADIUS)
authorize_check_query = "SELECT id, UserName, Attribute, Value, op \
  FROM ${authcheck_table} \
  WHERE Username = '%{SQL-User-Name}' \
  ORDER BY id"
authorize_reply_query = "SELECT id, UserName, Attribute, Value, op \
  FROM ${authreply_table} \
  WHERE Username = '%{SQL-User-Name}' \
  ORDER BY id"
```

Figure 8 Modify sql.conf in FreeRADIUS

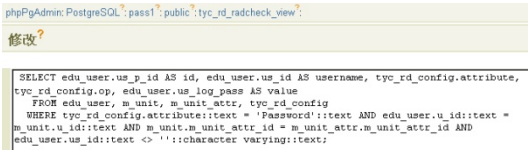

Figure 9 Set up PostgreSQL View data tables

To ensure our mechanism work stably, we build up two authentication encryption systems. While the first SSLVPN shuts down, the second one switches into Active state automatically in 3 seconds and users do not have to re-connect and can resume their operation. We also combine with the load balancing equipment. As the first connection breaks, the system can complete the flow guiding to the second connection in 3 seconds to resume normal operation.

In Figure 10, blue path is the encryption path. After finishing authentication, the encryption channel is established. At this time, the connection from the users wireless network equipment to the center-ends was completed encryption and we can ensure the security of user data transfer.

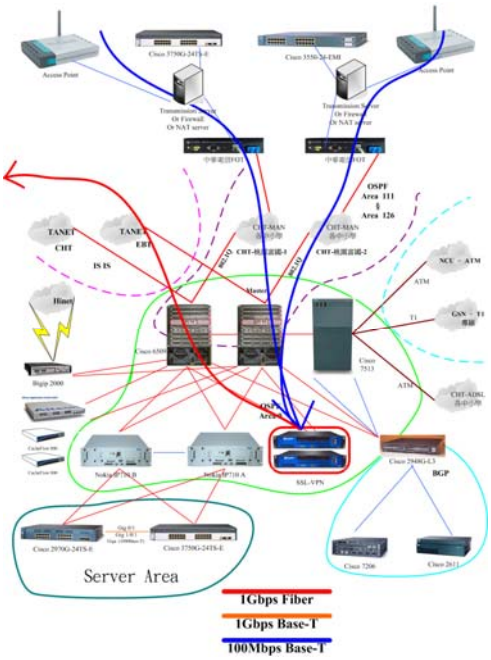

Figure 10

Encrypted VPN connection architecture

3.2 School-end Architecture

We build up the network diversion server at the school-end, and this server is located at the wireless network external connection point, as Figure 11. We can use FreeBSD attached with IPFW and Apache Web Service to activate the firewall. It can be implemented via using Linux OS with IP tables (netfilter) and Apache Web Service. We also can modify a general firewall which has the function of user certification to serve this task.

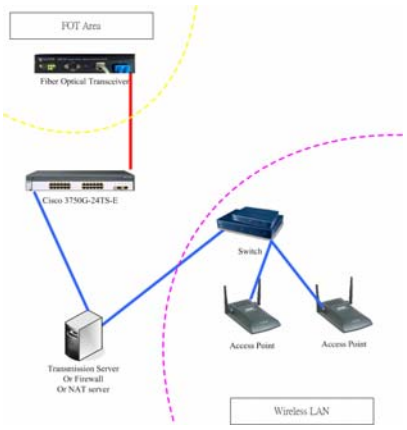

Figure 11 School-end Architecture

Taking Taoyuan County Network as an example, our diversion server adopts the transparent mode to allocate exclusive new wireless network Private IP at wireless network connected area. The advantages of this mechanism are that we don't occupy any established Public IP and don't need NAT service to avoid the poor performance of NAT. At the same time, we set the routing at

School-end and Center-end to ensure that only the user who completes certification can connect to Internet.

3.2.1 Set the Web Service on FreeBSD

We set Web Services on the server and set the index webpage automatically redirect to the SSLVPN website authentication systems, such as Table 2.

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<title>Document Moved</title>
<script type="text/JavaScript">
if (document.layers) {
document.write('<LINK REL=STYLESHEET HREF="authStyle_ns.css" TYPE="text/css">');
} else {
document.write('<LINK REL=STYLESHEET HREF="authStyle_ie.css" TYPE="text/css">');
}
setTimeout("goJump();", 1000);
function goJump() {
        top.location.href = "https://sslvpn.tyc.edu.tw";
}
</script>
</head>
```

Table 2 Webpage Redirection Setting

3.2.2 Set the IPFW on FreeBSD

The System activates IPFW mechanism to redirect external connecting flow to the local redirection website, as Figure 12.

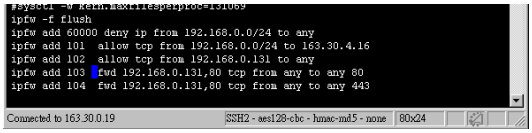

Figure 12 IPFW setting file

At Line 60,000, it means that there is no external connectivity in wireless network except Line 101 to 104. Line 101 permits the wireless network connecting to Center-end SSLVPN's IP. Line 102 allows the diversion server connecting to anywhere. Line 103-104 means redirecting the external website to the local redirection website.

4. System Testing

4.1 Connect to the Wireless Network

Connecting to the wireless base station with wireless network card tool, as figure 13.

Figure 13

Connect to the wireless network base station

4.2 Packet Intercept and Redirect in IPFW

When user opens any website for network connections with web browser, IPFW will direct the webpage to a web server redirection website, as Figure 14.

Figure 14 Redirection webpage

4.3 SSLVPN Certification Website

The users enter account and password to authenticate. At this time, the IP we allocated is a Private IP and the connection to Internet is not established yet, as illustrated in figure 15.

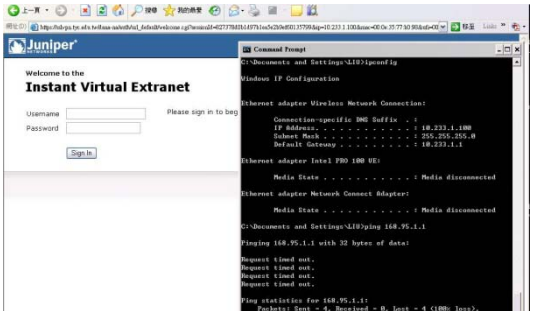

Figure 15 authentication webpage

4.4 SSLVPN System Certification

The system certificates account and password and establishes VPN connection, as illustrated in Figure 16.

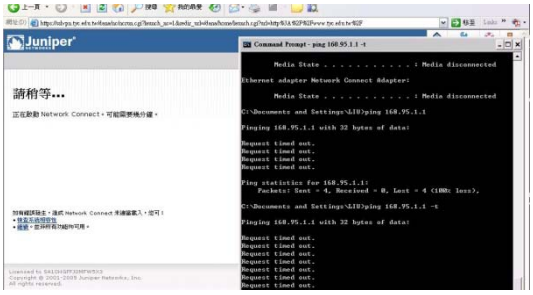

Figure 16 Establish VPN connections

4.5 Certification Completed

The VPN connection is established and the webpage will guide to the homepage of Bureau of Education Taoyuan County Government and the external connectivity is also established, as in Figure 17.

Figure 17

Complete the VPN Connections establishment

4.6 Examine IP Information Allocated by SSLVPN

We can use ipconfig command to examine the new IP allocated by SSLVPN, as Figure 18.

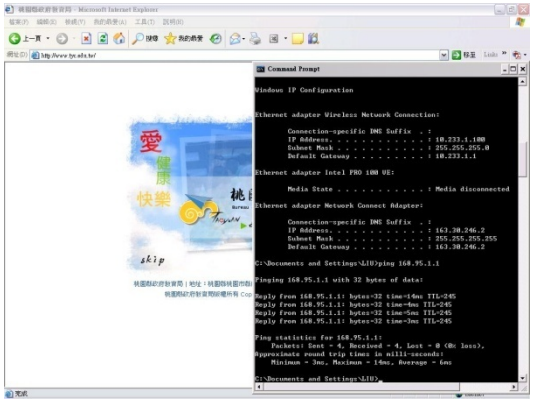

Figure 18 Examine the IP information

4.7 Certificate Oversea Connection

We connect to website (http://ipid.shat.net) to check certification, as illustrated in Figure 19.

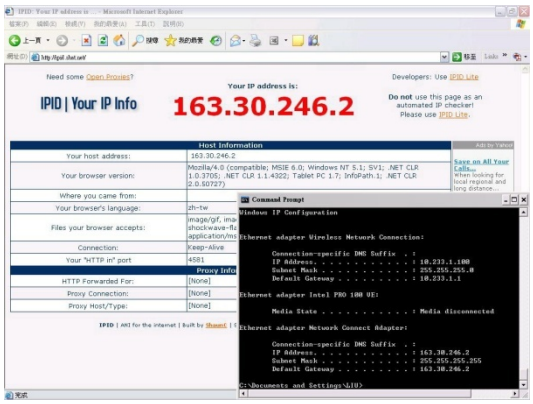

Figure 19 Certificate the IP we allocated

4.8 Install/Activate SSLVPN software automatically

We can install and start the SSLVPN client software automatically, which uses AES/SHA1 encryption method, LZO compression mode, and ESP transmission mode, as Figure 20.

Figure 20 The encryption software

5. Conclusion

The purpose of this study is to provide low-cost centralized authentication architecture and solve the problem of wireless encryption to improve the poor wireless network encryption mechanism at the same time. After successful certification, all connections are encrypted. We can control all Public IP allocated by wireless network effectively, and can adjust the size of exclusive segment of wireless network via use of wireless network.

Our achievement was used in elementary and junior high school campus wireless network owned by the Bureau of Education Taoyuan County. It allows every account to roam across the county and alleviates management pressure for the school managers. There is no restriction for brands of wireless base stations and network security-related settings, so we can build this mechanism more easily and at lower cost.

This mechanism can avoid abnormal network detection and meet the increasing growth of information security and confidentiality of information needs. We hope that this mechanism will become reliable wireless network security management and inter-school wireless network roaming mechanisms.

Reference

[1] Aggelou, George. Mobile ad hoc networks: from wireless LANs to 4G networks. *New York: McGraw-Hill*, 2005.

[2] Chen, Jyh-Cheng,Zhang, Tao,1962-. IP-based next-generation wireless networks. *New York: Wiley-Interscience*, 2004.

[3] Hardjono, Thomas. Dondeti, Lakshminath R. Security in wireless LANs and MANs. *Boston: Artech House*, 2005

[4] Janevski,Toni. Traffic analysis and design of wireless IP networks. *Boston: Artech House*, c2003.

[5] Raab, Stefan.Chandra, Madhavi W.Leung, Kent. Mobile IP technology and applications. *Indianapolis, IN :Cisco Press*,2005

[6] Stallings, William. Data and computer communications. *Upper Saddle River, N.J. : Pearson/Prentice Hall*,2004.

[7] Tse, David.Viswanath, Pramod. Fundamentals of wireless communication. *Cambridge: Cambridge University Press*, 2005.

[8] 楊士範。2004。CNET 電腦區。

[9] 蘇建郡、劉毓芬、楊凱宇。2002。校園無線網路認證系統之建置。TANET2002 台灣網際網路研討會。

[10] 蘇碩鈞、王唯至。2006。無線網路實務。iThome 企業採購特輯。