Security Mechanism for user access to Single SSID WLAN

Li Wang[1,2,4,*], *Mingshan* Xia[1,2,**], and *Fazhi* Qi[1,2,3,***]

[1]Dongguan Branch, Institute of High Energy Physics, Chinese Academy of Sciences, Dongguan Guangdong 523808, China
[2]Spallation Neutron Science Center, Dongguan Guangdong 523808, China
[3]Computing Center, Institute of High Energy Physics, Chinese Academy of Sciences, Beijing 100049, China
[4]University of Chinese Academy of Sciences, Beijing 100049, China

Abstract. Wireless local area network (WLAN) technology is widely used in various enterprises and institutions. In order to facilitate the use of users, they often provide a single SSID access point, resulting in different identities of users authenticated and authorized can connect to the wireless network anytime, anywhere as needed and obtain the same accessible network resources such as bandwidth, access control (ACL) and so on. Multiple SSID can solve the problem but it will be confused to users who don't know which SSID can be connected. Although we could prevent visitors from accessing intranet resources by isolating the wireless network from the internal network, this would make it impossible for users to use the wireless network for internal office work. In this paper, we propose an access control system that grouping users according to the different identities and users authenticated and authorized can access different network resources because a wireless access point dynamically maps an SSID provided by a mobile station to a BSSID based on a VLAN assignment. The deployment experiment of the solution proves that users of different identities accessing the same wireless network can set different access policies, which effectively improves the security of the wireless network and simplifies the management of the wireless network.

1 Introduction

With the development of computer network and wireless communication technology, wireless network technology has been widely used in various companies, enterprises and institutions. It's very convenient for users who can access the wireless network at anytime and anywhere after being authenticated and authorized. And different users with different identities will share wireless network in single such as bandwidth, accessible resources. However, network security problems will arise:When one's computer infected with a virus connected to the wireless network, it may cause the virus to spread throughout the network. At the same time, it may lead to personal information stolen, business data tampered, business data fraud, network paralysis, etc. and the loss is unpredictable. If different permissions cannot be assigned based on user identity, the network resources accessed are the same; Especially, if the

*e-mail: wangli320@ihep.ac.cn
**e-mail: xiams@ihep.ac.cn
***e-mail: qfz@ihep.ac.cn

internal network resources are exposed to visitors, the current network security equipment or functions will be useless, which will not only cause waste of investment, but also cause serious security incidents such as important data information stolen. It will lead to unreasonable allocation of bandwidth resources because network resources cannot be allocated according to user identity. When a user is threatened by security, it is bound to bring great impact on the whole network.

2 Related Works

In order to deal with various security threats in wireless network, corresponding wireless security technology came into existence, including media access control (MAC) filtering, service set identifier (SSID) matching, wired equivalent privacy (WEP), port access control technology (ieee802.1x), WPA (Wi-Fi Protected Access), WPA2, IEEE 802.11i, etc. [2].The efficiency of media access control(MAC) filtering method will decrease with the increase of the number of terminals, and illegal users can obtain the legitimate MAC address table through network interception, and MAC is easy to modify, so illegal users can steal legitimate users' MAC address for illegal access[2][3] . In paper [2], SSID setting can be used to group users well and achieve certain security by providing password authentication mechanism. In paper [4], once there is a network intrusion and the wireless network needs to be installed, SSID should be changed immediately to ensure the wireless network security. However, there are too many SSID Settings, so that users are confused and cannot distinguish which SSID they should access. In 2000, the popularity of Wi-Fi lans attracted the attention of the security and encryption community, which soon found defects in the WEP scheme[5]. By the end of 2001, the tools were available on the Internet, and it took only a short time to break through WEP. Port access control technology (ieee802.1x), WPA (Wi-Fi Protected Access), and IEEE 802.11i ensure the user access to the wireless network identity authentication security[2], but the same SSID user according to the user identity to achieve different access control policies, also can not achieve effective isolation.

3 Security Mechanism

The first question about access permissions is how to recognize user identity. And the second question about network resource division is how to assign user permission based on user identity. Our research is based on these two questions.

3.1 Grouping Users

There is a network access and control system in IHEP, in infigure1 we named it WebPortal server which offers registration service for users. Before access to wireless network, user should register first and they also will choose different identities such as student, staff, visitor. After the system admin approved, users will get their identities that achieves user grouping. As the infigure1 shows, when the user first requests to access the wireless network, it will be forced to request the WebPortal server for registration. The user choose the appropriate identity, fills in the equipment information and submits the form. Approval will be given by the appropriate administrator. After the approval, the grouping information of users identify and device information will be saved to database.

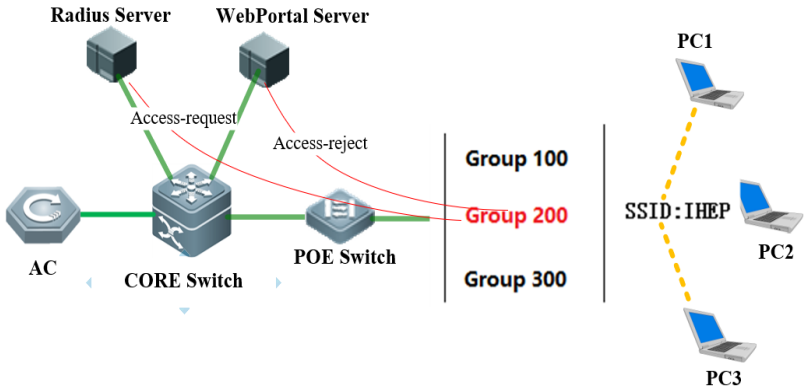

Figure 1: Authentication Process

We divide users into three categories, Staff users, visitor users and unauthorized users. Mobile terminals A, B, and C respectively represent users with different identities, and will be grouped in different groups after registration, so the grouping attribute table is shown in Table 1:

Table 1: Grouping Users

Devices	Identify	Group	BW	authority
PC1	Staff	Group100	50MB per second	Intranet or Internet
PC2	Visitor	Group300	120MB per second	Internet
PC3	unauthorized	Group200	default	No-access

3.2 VLAN

VLAN (Virtual Local Area Network) is a virtual local area network. It is an emerging switching technology that implements a virtual work group by dividing the devices in the local area network logically rather than physically. Using VLAN technology has the following advantages [6]:
1. Control broadcast storm
A VLAN is a logical broadcast domain. By creating VLANs, broadcasts are isolated, and the scope of broadcasts is reduced. Broadcast storms can be controlled. 2. Improve overall network security
According to the routing access list and address division principles, you can control user access rights and logical network segment sizes, and divide different user groups into different VALNs, thereby improving the overall performance and security of the switched network. 3. Simple and intuitive network management
For switched Ethernet, if network segments are reassigned to certain users, network administrators need to readjust the physical structure of the network system, and even need to add network equipment to increase the workload of network management. For a network using technology, a network user in different geographical locations can be divided into a logical network segment according to department functions, object groups, or applications. Workstations can be moved arbitrarily between workgroups or subnets without changing the physical

connection of the network. The use of virtual network technology greatly reduces the burden of network management and maintenance and reduces network maintenance costs. In a switching network, a flexible combination of network segments and institutions is provided. Our paper combines the advantages of VLANs and applies VLAN technology to wireless networks, and divides wireless networks into different VLANs. After one mobile device or computer connected to the SSID, it will be allocated into one VLAN due to the identity categories registered by the device. And the same identity will be allocated the same VLAN. Therefore different access policies can be set on different VLANs, for example: you can restrict network traffic, allow specific devices to access, and make specific ports to be forwarded. These effectively prevent illegal devices from undermining system security and illegally acquiring system data.

3.3 Authentication and Authorization

The RADIUS protocol is a dedicated authentication management protocol, which is called Remote Authentication Dial In User Service. At the transport layer, RADIUS packets are encapsulated in UDP packets, and at the network layer, they are encapsulated in IP packets. A retransmission mechanism is set to process packets that do not receive a response after a timeout. The NAS acts as a RADIUS Client and is responsible for collecting user requests and submitting it to the RADIUS Server. The RADIUS Server is like a database that stores a large amount of user information and configuration information of some access servers. It authenticates the transmitted information and returns it to the RADIUS Client, which controls the user's access to the network. To prevent someone from maliciously stealing the user's password, the information passed between the RADIUS Server and the RADIUS Client can be encrypted with MD5 to ensure security. The client and server share a private key to encrypt the data. The RADIUS authentication and authorization interaction process is shown in figure 2:
1.Enters a account and password and waits for the return result.
2.RADIUS client sends an access-request to RADIUS server according to user name, pwd and other information.
3.RADIUS server will compare and analyze the user information from database. It will send permission information (Accept, Reject) to the RADIUS client
4.RADIUS client accesses/rejects users according to the authentication result received. If the user can be accessed, the RADIUS client sends the
account-request package to the RADIUS server, and the status-type value is start.
5.RADIUS server returns accounting-response package;
6.RADIUS client sends account-request package to RADIUS server, and status-type value is stop;
7.RADIUS server returns account-response.
8.After RADIUS client receives account and pwd, it buids an access-request package and sends it to the RADIUS server.
9.Packet contains user name, pwd and other relevant information. The password is encrypted by MD5. If non-response for a long time and access request packet retransmitted several times, it will be considered as a server or network failure. The access request package will be sent to the alternate RADIUS server.

This article continues to use the RADIUS protocol for authentication and authorization. The traditional RADIUS authentication process is changed as shown in Figure 2. In process (1), the user no longer enters the user name and password, but uses the user device MAC address as the user name and password. Obtained automatically by the program. In the process

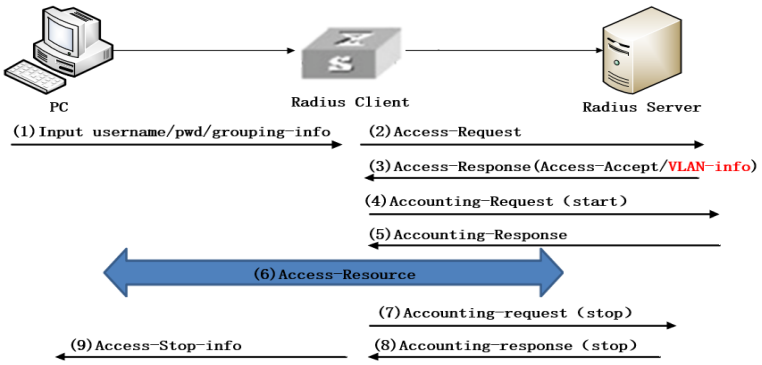

Figure 2: Authentication Process

(3), the user identity information and network configuration information are added to the original Users database. After the user requests, the RADIUS server compares and analyzes the user information with the Users database information. After the authentication is passed, the user is added to the response packet. Group VLAN number, and network configuration information. In the process (6), after obtaining the authentication response, the wireless controller divides the user into the corresponding VLAN according to the user group VLAN number. Users can access wireless network resources according to the corresponding VLAN policy.

3.4 Access Control

After the mobile device or computer connected to the wireless network, they will obtain different IP addresses because of identity categories, such as: the default device category, the assigned IP address is 10.202.1.0/24, and the employee class is assigned an IP address: 10.201. 1.0 / 24, the guest class is assigned an IP address: 10.203.1.0/24. Taking ACL technology as an example, data access control can be performed for different IP address sources. Employee users can only access the 192.168.1.0/24 address resource; guest users can only access the 192.168.3.0/24 address resource; the default Only the address resource of 192.168.2.0/24 can be accessed. The following are the wireless network access permission settings:
ip access-list extended acl
10 permit ip 10.201.1.0 0.0.0.255 192.168.1.0 0.0.0.255
11 permit ip 10.202.1.0 0.0.0.255 192.168.2.0 0.0.0.255
12 permit ip 10.203.1.0 0.0.0.255 192.168.3.0 0.0.0.255
13 deny ip any any
Therefore, after connecting to the same SSID, network devices of different identity categories will obtain different network access rights, different performance experiences, different data resources, etc., which ensure the reasonable allocation of network resources and the security of data resource access.

4 Testing Environment

We adopt an open source software Freeradius-3.0.10, which can be downloaded from the Freeradius official website (http://freeradius.org). The operating system uses the CentOS7 X64 version, which is directly installed through the yum command to build the radius server. MySQL used by background user data storage.
The Freeradius parameter contains VLAN attribute information. Since it is not added in the default attrs file, we cannot see the VLAN request information in the radius-X log. Therefore, we need to set Tunnel-Type (// represents the VLAN), Tunnel-Medium-Type (// value is 6, or IEEE-802), and Tunnel-Private-Group-Id (// VLAN to be issued ID) Three attributes are added to attrs.
The wireless network configuration is mainly divided into 5 parts, namely: creating a wireless network SSID; AAA authentication system settings; 802.1X authentication settings; wireless network device registration page; VLAN grouping function settings.

5 Conclusion

In our paper, we set three different VLANs in one SSID, and each VLAN with different bandwidth and access control policy. Figures 3, 4, and 5 show three wireless devices, which respectively represent three types of user groups. Users carry VLAN attributes vlan2001, vlan2002, and vlan2003. After authentication and authorization, they successfully access the wireless network and obtain different network configurations such as IP addresses. They are 10.201.1.2, 10.202.1.2, and 10.203.1.2. By connecting different VLANs, this solution can achieve different access control for different identity users on a single SSID wireless network, bandwidth, enhance network security, and facilitate wireless network management.

```
Total Sta Num : 401
STA MAC        IPV4 Address    AP                                  Wlan Vlan Status          Asso Auth      Net Auth       Up time
-------------- --------------- ----------------------------------- ---- ---- ------------- -------------- -------------- ------------
e446.da40.22b2 10.201.1.2      CSNS_A1_F3_AP05/1                   4    2001    6.5M/D/bgn   WPA_1X         OPEN            0:00:00:07
CSNS-WIFI-WS5708-1#
```

Figure 3: Group 200

```
Total Sta Num : 396
STA MAC        IPV4 Address    AP                                  Wlan Vlan Status          Asso Auth      Net Auth       Up time
-------------- --------------- ----------------------------------- ---- ---- ------------- -------------- -------------- ------------
e446.da40.22b2 10.202.1.2      CSNS_A1_F3_AP05/2                   4    2002  144.5M/D/an    WPA_1X         OPEN            0:00:00:21
CSNS-WIFI-WS5708-1#
```

Figure 4: Group 300

```
Total Sta Num : 402
STA MAC        IPV4 Address    AP                                  Wlan Vlan Status          Asso Auth      Net Auth       Up time
-------------- --------------- ----------------------------------- ---- ---- ------------- -------------- -------------- ------------
e446.da40.22b2 10.203.1.2      CSNS_A1_F3_AP05/2                   4    2003  117.0M/E/an    WPA_1X         OPEN            0:00:00:46
CSNS-WIFI-WS5708-1#
```

Figure 5: Group 100

References

[1] Zhang bo, Gao Song,Analysis of Wireless Network Security Technology [J] *Information Security*

[2] Wu Xianping. Design and implementation of campus network user identity authentication based on 802.1x[J] *Manufacturing Automation*

[3] Meng Min,Design and implementation of campus network security authentication based on 802.1x protocol[J],*Electronic Design Engineering*

[4] HAN Dongsheng, HAO Conghui, CHEN Zhixiong. A User Selection Algorithm Based User Grouping for The Heterogeneous Network[J], *Journal of Harbin Engineering University*

[5] Liang Feng Shi Xingrong Qu Fuping Enhancing the Security of WLAN Based on Combining 802.1x Authentication and WEP, *Computer engineering and technology*

[6] FENG Dong-zhu YANG Deng. Based on VLAN technology in campus network construction[J], *Microcomputer Information*