Research and Mass Deployment of Non-cognitive Authentication Strategy Based on Campus Wireless Network

Dapeng Huangfu[1], *Xiaoping* Tian[1], *Xingjian* Wang[1], and *Ping* Chen[1,·]

[1]Center Information & Network Technology, Beijing Normal University, Beijing, 100875, China

Abstract. With the rapid development of Internet +, the dependence on wireless networks and wireless terminals are increasing. Campus wireless network has become the main network of teachers and students in campus on the internet. As there are uneven clients and a wide variety of intelligent terminals now. Simplified authentication and network security become the most urgent problem for wireless network. This paper used the Portal + Mac authentication method to realize the non-cognitive authentication of teachers and students on basis of the analysis of the advantages and disadvantages of mainstream authentication of campus wireless network, such as 802.1X authentication, Portal authentication, Mac authentication and DHCP authentication. Teachers and students only need portal certification at the first time, then surf the internet with non-perceived authentication at the second time and later. This method increases network security, and is better to meet the needs of teachers and students.

1 Campus wireless network authentication mode analysis

With the rapid development of Internet+ and the popularity of intelligent terminals, the dependence on wireless networks and wireless terminals are increasing. Teachers and students hope to easily access the network anywhere in the campus. In recent years, with the rapid development of 5G wireless network technology, the construction of wireless network in colleges and universities have been completed, and the basic construction of campus wireless network have been completed. How to provide convenient and safe authentication method to users is one of the important research topics in wireless network construction [1].

At present, in the campus wireless network environment, the mainstream authentication method are 802.1x certification, Portal certification, DHCP access certification and Mac address certification.

1.1 802.1x certification

The IEEE 802.X protocol has a more complete authentication function, by controlling the port limit of the Ethernet access device to the non-certified user[2,3]. In the cable network,

· Corresponding author: chenping@bnu.edu.cn

the 802.1X protocol divides the switch port into a physical port and a logical port. The logical port is closed without authentication, and only EAPOL data packets can be passed. After the successful authentication, the logical port opens and allows the normal data package to pass. Cable network users mainly use windows operating system. It needs to configure the client or install terminal software, bring greater challenges for ordinary users.

In the wireless network, the wireless handheld terminal are mostly integrated with the 802.1x client. Users only need to fill in the account and the password which could be realized. After the first successful certification, the authentication terminal would automatically log on. This process realized the non-perceived authentication based on 802.1x. But the terminal compatibility was poor. The operating systems such as windows XP and windows 7 still needed to install software or configure clients. At present, all colleges and universities are using a SSID-Mobile signal, mainly providing service for mobile terminals. At the same time, global alliance signal Eduroam is also based on the 802.1X protocol.

1.2 Portal authentication

Portal authentication [3,4] is one of the most popular authentication methods, and its compatibility is better. After the user access the wireless network to obtain the address, the gateway would be able to redirect the non-certified user to the Portal authentication page, and then access the network resources after the success. Portal could achieve network access and release, but there was a difference between the way and the mechanism.

At present, there were three main types of Portal authentication. (1) Two times authentication. The first authentication through AC Portal could achieve the access and users could access the campus resources. The second authentication could be realized by the Portal authentication billing system, and the user could access the outside network resources. The tedious process of 2-time authentication process reduced the efficiency of the network and the user experience. (2) One time authentication. After AC Portal and certification billing system Portal docking, users could connect to AC. The billing system would give a response to the AC authentication request, while AC Portal carried the account and password to the certification billing system to send a request. Simultaneously the certification billing system issued the strategy to the server, in order to realize the user's accurate release. AC Portal achieved the user access, and one time authentication could achieve access and release. This authentication could simplify the user authentication process. But each manufacturer's AC needed to meet with the billing system to achieve the docking debugging, so the backstage maintenance was very difficult. (3) The independent Portal server. An independent Portal server was set up in the wireless core switch and the campus exit. It was used to realize the access of wireless network, and the release by the Portal sever of the linkage authentication billing system at the same time. This authentication solved the difficulties of docking between different manufacturer controllers, and it was more convenient to maintain. But the wireless network needed to adjust the topology and increase the Portal server.

The Portal authentication had several problems: (1) Users need to have the active authentication each time and it could not achieve no perception; (2) This authentication could not get the user Mac address. The user's identification was not accurate, so the user with the same IP address would be treated as the same user in a short time.

1.3 Mac address authentication

The Mac address authentication was based on the EAP authentication protocol framework, which was matched by the Mac address of the terminal equipment to the user[4]. Network

managers needed to maintain a Mac address list to record all terminal Mac addresses that accessed to the network. When the user accessed the network, the Mac address of its terminal would match the address in the Mac address table firstly. Only the successful matching terminals were allowed to access the network. This authentication had several advantages. It was convenient, fast, more practical, adapt to small-scale wireless network environment or a few special users under the large-scale wireless network. But it also had few shortcomings. This authentication needed administrator to bind the terminal Mac address and user information and record to the authentication server. It would undoubtedly be a disaster for a large-scale network environment and the maintenance work would be more than imagination. In addition, this method had the risk of forging the Mac address. The user's network flow would be stolen easily, and the network security had some risks.

1.4 Non-perception authentication with the combination of Portal and Mac

The non-perceived authentication with the combination of Portal and Mac addresses overcame their shortcomings and retained their respective advantages [4,5]. The first certification was realized through Portal authentication, and completed the binding work of accounts and terminal Mac address. After the authentication, users could login on the network when the terminal Mac and the Mac address table matched successfully. Users did not participate in this process, while AC completed the automatic certification initiatively. At present, there are differences in the network mode of various colleges and universities. The realization form of Portal and Mac was different, but the principle was the same. So this method was relatively perfect and feasible.

Through the study of the above four authentication methods, the terminal adaptability of the 802.1X certification was not suitable for the popularization of the masses. The complexity of the Mac address authentication operation was not suitable for independent deployment. Portal certification required certification every time and was so inconvenient. Only Portal and Mac were integrated address authentication methods, which had the implementation and convenience, were suitable for large-scale application and deployment.

2 Methods of no sense of authentication

The original authentication methods of the wireless network of Beijing Normal University is the 802.1X certification, BNU-Mobile (the mobile phone and the flat terminal), Portal certification: BNU (Teaching area), BNU-Student (Dormitory area). In order to facilitate users to use the free resources on campus and IPv6, the Portal had only been enabled the access function. But there was safety problems.

2.1 Non-sensory authentication topology

As the wireless network became the main Internet way and the country's attention was drew to the network security, it was imperative to enable Portal access certification [6-10]. In order to implement the deployment of Portal access, and to improve the experience of the Internet, the combination of Portal and Mac were used in the whole school. The whole authentication way was made up of the following parts, as shown in figure 1:

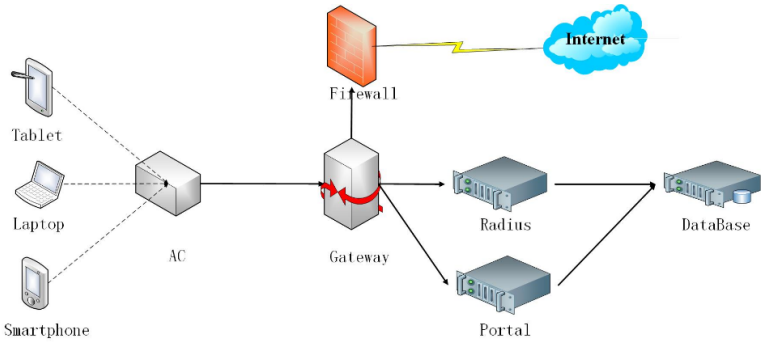

Fig. 1. Mac and Portal no-cognitive authentication logic diagram.

1) The user terminal were usually a notebook, intelligent mobile phone, tablet and so on with the installation of the browser terminal. These terminals contained wireless network card. The browser was used to trigger Portal authentication, and the network card provided the only user Mac address.

2) As a wireless user access gateway, AC equipment carried several functions. The first was the security access function, which was responsible for access to the user's legitimacy detection. The second was pushing Portal certification page for the user terminal. The third was the linkage line function. AC would kick the user while the wireless terminal was off the wireless network or the long-term no traffic. At the same time, the billing system linkage kicked off the user after received the offline information. If the billing system had long-term non-flow and then kicked off the terminal, AC would kick off the user after receiving the information.

3) Portal server was the user authentication entrance. The user terminal first accessed to the wireless network, the AC re-directional web interface to the corresponding billing Portal server. It would push the web authentication page to the user terminal based on the HTTP protocol and submit the information containing the user account/password to the billing database.

4) RADIUS server could achieve certification, authorization and accounting services, which was usually considered as the AAA server. It had four functions as the scalability of the RADIUS. The first function was responsible for receiving information of Portal server and AC device, such as user name/password, Mac address, online time and flow, etc. It realized the user authentication after comparing these information with the billing database. The second was sending the control strategy of users to AC device, and authorizing the user terminal online (offline) certification request. The third was accounted based on the user's online time or flow. The last was binding the user Mac address and user account (first automatic binding), and storing the user terminal information into the billing database.

5) Billing database was responsible for user terminal information, corresponding relationship of account and Mac address, and authentication billing data storage.

2.2 Non-perceived authentication process

The non-perception of the combination of Portal and Mac was in application in Beijing Normal University. The first certification achieved access and accuracy through the Portal certification. At the same time, that certification achieved the binding of the user account and the Mac address, and storing into the billing system. The authentication realized the user's access and accuracy certification by comparing the Mac address in the terminal and billing system Mac table. The whole process was initiated by AC, cooperated with the

completion by Radius and the billing system database. The user had no sense of authentication, so it was called non-perceived authentication.

The specific authentication process was shown in figure 2.

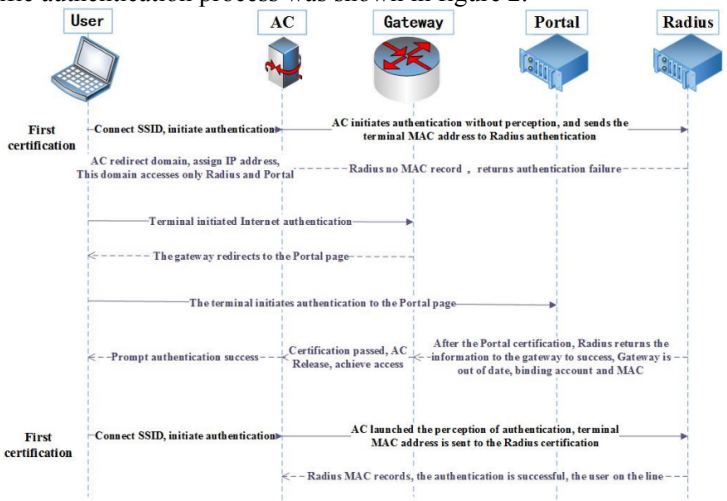

Fig. 2. Non-perceived authentication process.

(1) When the user connected to the SSID firstly, the user terminal initiated an authentication request to AC. AC got the Mac address of the user terminal and initiated the Mac authentication request to the RADIUS server. At this time, the Mac address of the user terminal was not recorded in the billing database connected by the RADIUS server, so it would reject the authentication, and the Mac address authentication failed. AC would re-assigned the user to the Guest VLAN for the next certification.

(2) AC took the initiative to push portal certification page after Guest VLAN opened Portal certification. In other case, the terminal send HTTP requests to AC when a user visited a web site, and AC would redirect the user's HTTP request to the Portal authentication page. The user could complete the Portal authentication on the portal page, while the Radius server was bound to the user's account and the Mac address.

(3) After the successful Portal certification, the user could access the network normally. The first certification is the regular Portal authentication.

(4) When the user connected to the SSID, the AC sent the Mac authentication request to the RADIUS server firstly. As billing database corresponding to the RADIUS server had the user's account, Mac address and other information records, the authentication would be successful and the user would be on line without the Portal certification. The following-up authentication was completed by the terminal, AC, and RADIUS server automatically, which did not need users' participation. So it was no sense to the user.

From the authentication process, the non-perceived authentication was not free of certification, which was to reduce the user's participation in the authentication process, and reduce the complexity of the operation. The non-perceived authentication was completed with no sense of perception, both guaranteeing the online security management, and improving the user's Internet experience. This authentication was suitable for teachers and students' wireless network service in campus.

3 Large-scale deployment of non-perceived authentication

Portal and Mac authentication combinations were relatively mature for non-sensory authentication tests and small-scale cases [4]. But in the process of mass deployment, it

would meet the problem of software and hardware bottlenecks and the adaptability of users. The work that needed to be prepared in advance included:

(1) Billing strategy adjustment

(2) Portal and Radius server: Portal service used Apache software to realize the function. As the Apache service's bottleneck, it did not respond to the problem when the number exceeded 10000. Therefore, it was necessary to calculate the number of Portal and share the pressure on multiple Apache servers before a large-scale deployment. The wireless online users of Beijing Normal University would exceed 30,000 in the rush hour. However, the Portal page request was not more than 20000. We had set up 2 Apache servers, the dormitory area and the teaching area of the wireless Portal certification respectively. Then, the Portal certification page requested no more than 10000, and the controller had no pressure in general.

(3) Wireless controller: Previously, the controller system needed to be upgraded to the latest stable version, which was used to solve the controller version and enhanced the performance of the controller. At the same time, the configuration of the user without traffic offline and the linkage line was build, preventing the terminals of users to take up the charge and send a number. It was recommended that the HTTPS protocol be closed, because the protocol could lead to an Apache pressure, while the controller's CPU would be consumed by the agreement.

(4) Billing database optimization: The campus wireless network of Beijing Normal University configured a VLAN address pool in the teaching district and the dormitory area. At the same time, the user terminals could achieve cross-controller roaming. Therefore, the IP address obtained by the user terminals would not change. The billing system would generate online logs only when the user was active or long-time no traffic was forced to get off the line. So, the users produced only a few online logs every day. When the Portal authentication and the Mac authentication were not cross-controllers, the billing system would produce a web log when the teachers or students cross the controller. In this case, the billing system would produce a large number of web logs a day. So many web logs would generate great pressure to the billing database.

4. Conclusion

The coexistence of wired and wireless network is the trend of campus network construction in the future. The combination of MAC and Portal technology is the security of MAC address authentication and the security of Portal authentication. This integrated authentication for the flow or length of billing colleges and universities, that is to protect the legitimacy of users, but also to avoid the use of non-perception of authentication methods resulting in unknown traffic or economic losses.

But this authentication method also has some disadvantages, although it can bring convenience to users, but if there is no limit to the number of user terminals, it will inevitably lead to the number of terminals flooding. According to each user will generally hold computer, tablet and mobile phone 3 terminal equipment to consider, in accordance with the user terminal number of Beijing Normal University Teachers and students were 3 and 5, the subsequent terminal access to campus network Radius with terminal access to campus network order kicked off the front of the terminal.

References

1. Xie Sheng jun, Yin Feng, Zhou Xu chuan. Cable and wireless integrated flat campus network design. Journal on Communication, **9**, 80-81(2013).

2. Long Jun jun, Yuan Aimin. ANRD-DPM Algorithm Based on MAC Certification and AS Level Related Decomposition. Bulletin of Science and Technology. **9**, 131-134(2016).
3. Steven K. Brawn, R. Mark Koan, Kelly Caye. Staying secure in an insecure world: 802.1x secure wireless computer connectivity for students, faculty, and staff to the campus network. Proceedings of the 32nd annual ACM SIGUCCS conference on User services. **4**, 273-277(2004)
4. Feng Lei, Lin Chunjian, Zhao Jun. Research on the technology of certification without perception based on MAC with Portal. Journal of Central China Normal University (Nat. Sci.), **5**, 4-8 (2017).
5. Wang Dao jia, Ma Yan, Huang Xiao hong. Research of DHCP based campus network admission control and senseless authentication method. Hua Zhong Univ. of Sci. & Tech.(Natural Science Edition). **10**, 181-185(2016).
6. Amna Saad, Mohd Izzat Mohamat Roseli, Muhammad Saufi Zullkeply. A smart e-voting system using RFID authentication method for a campus electoral. Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication Publisher: ACM.**14**, (2014).
7. Li, X., Yuan, H., Xiaofeng, C., Xinyi, H., Ticket-based handoff authentication for wireless mesh networks journal of Computer Networks.**73**, 185-194 (2014).
8. S. T. Ali, V. Sivaraman, and D. Ostry. Secret key generation rate vs. reconciliation cost using wireless channel characteristics in body area networks. 2010 IEEEIFIP International Conference on Embedded and Ubiquitous Computing. 644–650(2010).
9. Li, C., Nguyen, U.T. Fast Authentication for Mobility Support in Wireless Mesh Networks. Intconfof WCNC. 1185–1190(2011).
10. Yi, P., Wu, Y., Zou, F. and Liu, N. A Survey on Security in Wireless Mesh Networks. IETE Technical Review.**27**, 6–14(2010).