

Analysis of WIFI Wireless Network Security Scheme in Campus Environment

Youwu Liu

Sanming Institute of Modern Education Technology Center, Sanming, Fujian 365004, China

Abstract

Due to social and economic development, China's information technology industry has also developed rapidly, bringing great convenience to people's lives and work. The Internet has become an indispensable content in today's society. Its convenience and effectiveness determine its own important position. In the campus environment, wireless networks affect the learning and life of teachers and students. The author mainly analyzes the wireless network and its security scheme in the campus environment, aiming at promoting the development of wireless network security on the campus.

Keywords

Campus environment; wireless network; security scheme; convenience.

1. Introduction

According to relevant investigations and researches, not only Internet users in the global scope but also in China like to choose to use the wireless network to access the Internet. This shows that the wireless network has become a very popular part of people's access to the Internet. Campus-wide wireless network settings are an important point in the current impact on school education. Many teachers and students need to access the required information through wireless networks. Therefore, the security of WIFI wireless networks in the campus environment is an important part of the harmonious development of the school.

2. WIFI wireless network overview

Wireless networks and wired networks have a great degree of similarity to some extent. Within the scope of a building, wireless network devices are typically wireless network cards, access points, and computer adapters. The functions that a wireless network access point can perform are very similar to the switch-related functions in a limited network. In the limited network, Ethernet belongs to a more mainstream type of LAN technology. The development of this technology and the wireless network standard are carried out together, and the future development direction of the wireless network is also determined.

Due to the high popularity of wireless networks, many schools are gradually investing funds and human resources in the construction of campus network platforms. Therefore, the development of campus wireless networks has attracted the attention of schools. Many schools consider the issue of network security and begin to build their own internal local area network on campus. This will not only facilitate the use of teachers and students, but also improve the security of the network.

3. Second, the WIFI wireless network security program design in the campus environment

3.1 Technical aspects

Because of the continuous development of Internet technology, many inherent wired network access systems cannot meet the actual needs of most users for broadband services. Therefore, in order to meet the needs of customers, the wireless access system expands from the original narrowband to broadband, and faces data, and converts multimedia-related services. For most customers, their main concern is how to reduce costs and get high-quality services. At present, broadband wireless access technologies include high-frequency broadband, wireless frequency bands used in mid-band broadband mobile phones, and the like. First, the frequency spectrum of high-frequency broadband itself is relatively more voluntary, and its transmission rate is high. However, because it works in millimeter waves, it is easily affected by the weather. This type of access is generally used by communication operators. Secondly, the band of broadband in IF is better in transmission performance, and the actual coverage is wider. The related technologies are relatively mature, and they are highly competitive. In the current market situation, it is an ideal wireless access. The method is suitable for use in large-scale cities. Here, the radio interface related technology of the wireless frequency band used by Bluetooth can effectively provide bidirectional short-range communication between different devices. Bluetooth technology devices are cheap to use and small in size. In addition, some of the overall networks built using Bluetooth are relatively low-cost in terms of laying cables. Mobile phone Bluetooth technology is the most widely used among mobile phone users.

3.2 The construction of wireless networks

The construction of the wireless network needs to involve the design of the architecture and the core configuration. First of all, the systematic scheme of the wireless network constructed within the campus environment mainly uses the wireless switch plus "thin" AP mode. The actual coverage range is all the campus's teaching and administrative areas. The wired core switches and the Layer 2 switches that have been installed in the campus can successfully implement network connections with the help of Gigabit fiber. The following figure 1 is a network topology diagram. According to Figure 1, we can see that the campus cable network is partially composed of the exits of two routers, and the core part is a five-tier three-tier switch. In addition, an authentication server is connected in series. All users in this network must pass authentication servers before they can successfully access external network resources.

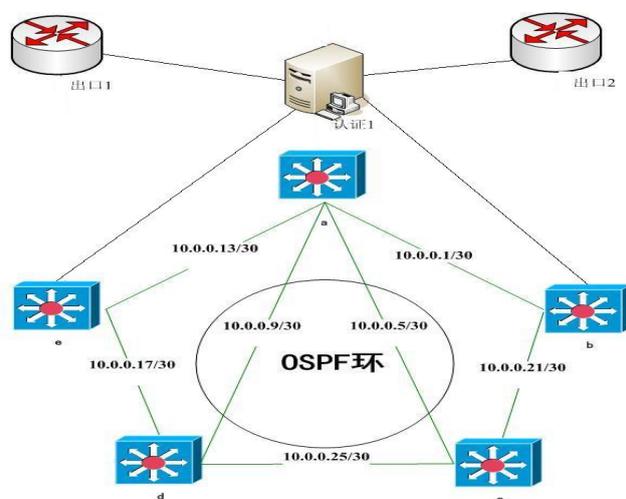


Figure 1 Topology

The wireless controller in the campus wireless network needs to determine its placement position according to the topology. The ospf routing protocol is used throughout this network, and the smallest

metric is considered to be the shortest path. The smaller the measure, the more likely that the link is selected as a route. After the completion of the wireless controller placement task, the placement problem of the wireless device under the core switch a is as shown in Figure 2 below.

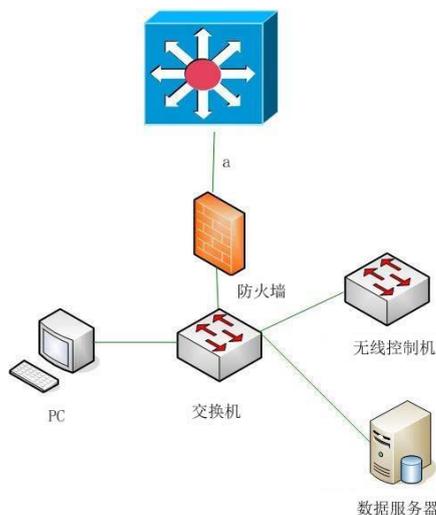


Figure 2 Wireless Network Structure

According to Figure 2, we can see that there is a firewall behind the three-layer switch a. The main role of the firewall is to prevent hacker attacks on the campus network, and to a certain extent can effectively limit some internal personnel access to the switch. Therefore, the firewall can create a relatively safe environment for campus wireless network security. After the firewall is connected to the second floor switch, the switch to work out two optical jumpers, one of the optical jumper connected to the data server, and another optical jumper to the wireless switch. In addition, the technicians also need to successfully configure IP addresses for the two machines. Using the IP address of the private network can effectively prevent malicious attacks from computers on the network external network. The two devices can also achieve mutual access. The wireless network control software is directly installed on the data server, and the wireless switch can successfully transmit some real-time data to the data server, and the related management personnel can easily control the wireless network. In addition, in order to effectively protect the wireless controller and other related equipment, the staff can configure the virtual local area network (VLAN) on the three-layer switch in time. The main role of the local area network is to successfully divide the equipment of the local area network into a single network segment. Virtual work-related data exchange technology.

4. Design requirements for wireless network security solutions

In the campus environment, the design of wireless networks is mainly to solve the problem of colleges and universities for wireless networks covering the campus. After the project is completed, students, staff, and staff can use the campus network to work. In addition, the design of the campus wireless network can improve the overall teaching quality in a timely and effective manner. Students' extracurricular life is more colorful due to the wireless network. The realization of the wireless network can also add points for the overall image of the campus, solve the problem that it is difficult for the limited network to fully cover the campus, and can meet the needs of the campus for temporary activities. The benefits for the development of the campus are numerous.

Wireless network design has the following characteristics in principle: First, campus wireless network design needs to be economical. The economic requirements of the program to use low-cost to get better performance, the relevant state departments require that the construction of the campus should be properly reduced some unnecessary investment, so as to avoid waste; Second, mobility. Mobility mainly meets the user's temporary use problem, which is an important advantage of the campus

wireless network; again, security. Wireless networks do not need to use cables for transmission. Therefore, the encryption of wireless networks has become an important issue that affects the security of campus networks. The design of campus wireless networks needs to effectively integrate products and security technologies to meet customer security requirements, and to solve campus network fluctuations and bandwidth, etc. within the maximum limit. Finally, developmental. In the era of informatization development, wireless network technology has developed at an extremely fast pace and technology has constantly been updated. Therefore, during the construction of a campus wireless network, the actual service life of the system should also be considered, and some new technologies are effectively used in the system. If the campus wireless network installation system is difficult to adapt to the future development, it will easily lead to repeated investment and waste of resources.

In addition, there are certain requirements for the distribution of users in the campus wireless network design. In the specific design process, the staff should set the number of wired points according to the flow conditions. Students return to the dormitory after class, the use of the network increases, and the pressure of traffic increases. Therefore, in the process of designing the project, the staff must not only ensure the actual availability of related equipment, but also need to improve the self-compression capability of the network equipment in time, so as to effectively mitigate the packet loss phenomenon under high load conditions. For areas where traffic is relatively unfocused, including cafeterias, it is also necessary to consider wireless coverage within the design of the plan.

5. Analysis and Test of WIFI Wireless Network Security Solution in Campus Environment

Table 1 below is a table of analysis of WIFI wireless network security solutions in the campus environment, as shown below. The WEP encryption scheme is an important part of it. WEP is the first security protocol in the wireless LAN. However, the security protocol is questioned because the cracking process is very simple.

Table 1 Wireless Network Security Solution

Encryption mechanism	Keys	IV	Encryption Algorithm	advantage	Shortcomings
WEP	Static 40 bits; 128 bits	24	RC4 algorithm	Under this encryption mechanism, users are allowed to obtain network licenses with the same encryption key and AP key, which can effectively prevent illegal access.	The security performance can not meet the requirements, the key can be easily cracked
TKIP	Dynamic 128-bit	48	RC4 algorithm	In the case of software upgrades, the practical application of the mechanism improves and network security improves.	Security does not meet requirements, easily cracked
CCMP	Dynamic 128-bit	48	AE5 algorithm	High safety performance	High degree of hardware requirements, difficult to implement, and the application process is subject to certain restrictions

After the campus's wireless network system was successfully built, students' growing Internet access requirements were met and the school was able to effectively use the wireless network to monitor the overall situation of the school and handle it in a timely manner in the event of a failure. Whether the security of the wireless network scheme meets the requirements is an important one related to the design and implementation of the scheme.

5.1 Test environment

First, the hardware is: a wireless switch, four wireless access points, a server, and two laptops. In addition, the software part is the notebook computer operating system (Windows XP) and the server computer operating system (Windows 2003 server).

5.2 Performance testing

The campus wireless WIFI performance test is also an important part of the entire quiz. First, the network supports Web-based authentication. The main test goal is to verify that the network supports valid Web browser-based authentication. Second, the quiz supports multiple authentication methods for different SSIDs. Probing devices include wireless switches, APs, and Laptops. The environment for the test is that after the wireless AP is connected to the layer 2 switch, it directly connects to the campus network through the layer 3 switch and is directly connected to the authentication server. Figure 3 shows the topology of the test, as shown below.

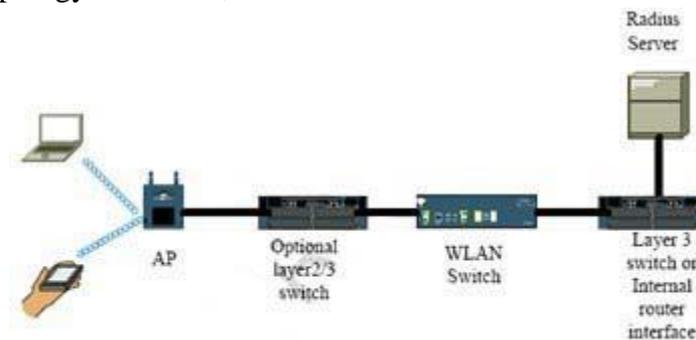


Figure 3 Test topology

Quiz process: Set different SSIDs on one AP and use different authentication and encryption methods for authentication; verify that related wireless clients can connect to three of them. The results of the quiz show that: Key users can search for wireless network signals, display SSIDs wireless1 and wireless2, and can successfully connect to external networks. The test is successful.

In addition, the test process also involves bandwidth control. The purpose of the test is to verify that the system can successfully provide bandwidth control for different levels of customers. The test equipment is wireless switches, APs, wireless terminals, and Radius servers. The test environment is as follows: The AP is connected to a Layer 2 switch and the Layer 3 switch is used to communicate with the wireless switch. The test procedure is: set a wireless network named guest as an open system, and additionally set the wireless network as a student to be static WEP authentication; limit the speed to 1 Mbps for the guest; use the laptop as a guest to access the wireless network; confirm the bandwidth The highest value. The test results showed that the actual downstream flow was 65 k/s. After the shutdown limit was reached, the flow rose to 1.5 M/S.

5.3 Campus Wireless Network Security Technology

The development history of campus wireless network security technology relates to the key content of school education development. Among them, VPN technology belongs to a kind of virtual private network. It refers to an important technology that can continuously realize the security development of campus wireless networks through some related encryption technologies and special channels on the public IP network platform. It can also limit the access to related resources and significantly increase the security of wireless networks. In addition, wireless network security technology also involves a

filtering part. This filtering technology is called MAC. The technology can establish a specific MAC network card to access in the setting of the router, reject other types of MAC addresses to send any information to the device, and protect the safe operation of the campus wireless network.

6. Conclusion

The author mainly discusses the specific situation of the campus wireless network, analyzes the campus WIFI wireless network design and security plan, and aims to help improve the campus wireless network security development.

Acknowledgements

Fund Project: Funding Project of Sanming College Scientific Research Fund Project (B201312/Q) in 2013.

About the author: Liu Youwu (1983-), male, from Sanming City, Fujian Province, mainly engaged in computer and network technology research.

References

- [1] Zhang Tao, Liang Songtao. Wireless network retransmission technology based on network coding [J]. Computer Engineering. 2013 (08).
- [2] WANG Wanliang, ZHANG Xiaohuan, YAO Xinwei, XU Yuefeng. Adaptive TFRC Mechanism Based on Streaming Media Transmission in Wireless Networks [J]. Computer System Application. 2013(07).
- [3] Liu Yonghua, Zhang Fengqing. Computer Networking and Maintenance Technology [M]. Tsinghua University Press, 2006
- [4] Wang Hao, Chen Changjiang, Radar, Gao Peng, Liu Jian. Design of EMU debugging platform based on wireless network environment [J]. Computer Measurement and Control. 2013 (04).
- [5] Long Fei, Wang Chunqi, Yang Zhian. Routing and Channel Allocation in Directional Antenna Wireless Networks [J]. Journal of PLA University of Science and Technology (Natural Science). 2013 (02).
- [6] Fan Yongjian, Chen Hong, Zhang Xiaoying. Wireless Sensor Network Data Privacy Protection Technology [J]. Chinese Journal of computers. 2012 (06)
- [7] Xia Xiukun. Design and Implementation of Wireless Campus Network Based on IEEE802.11 [D]. Hebei University, 2011

Mailing address: Teacher A-207, Sanming College, No. 25 Jingdong Road, Sanyuan District, Sanming City, Fujian Province, China. Address: Liu Youwu, Tel: 13950960786 Zip Code: 365004