

Design and Realization of Wireless System of National Engineering and Technology Library

Ye-Yang ZHANG^a, Lin MU^{*} and Yang HAN^b

Institute of Scientific and Technical Information of China, Beijing100038, China

^azhangyy@istic.ac.cn, ^{*}mulin@istic.ac.cn, ^bhany@istic.ac.cn

Keywords: Wireless system; Cybersecurity law of the People's Republic of China; 802.11ac.

Abstract. Based on the needs of the wireless system of the National Engineering and Technology Library, according to the latest requirements of the Cyber Security Law of the People's Republic of China, and combined with the latest achievements of wireless technology development, the wireless network of the National Engineering and Technology Library has been redesigned and constructed. The new wireless network has greatly improved the transmission rate, security, unified management convenience and wireless network authentication access convenience, which provides a guarantee for providing better network service.

Introduction

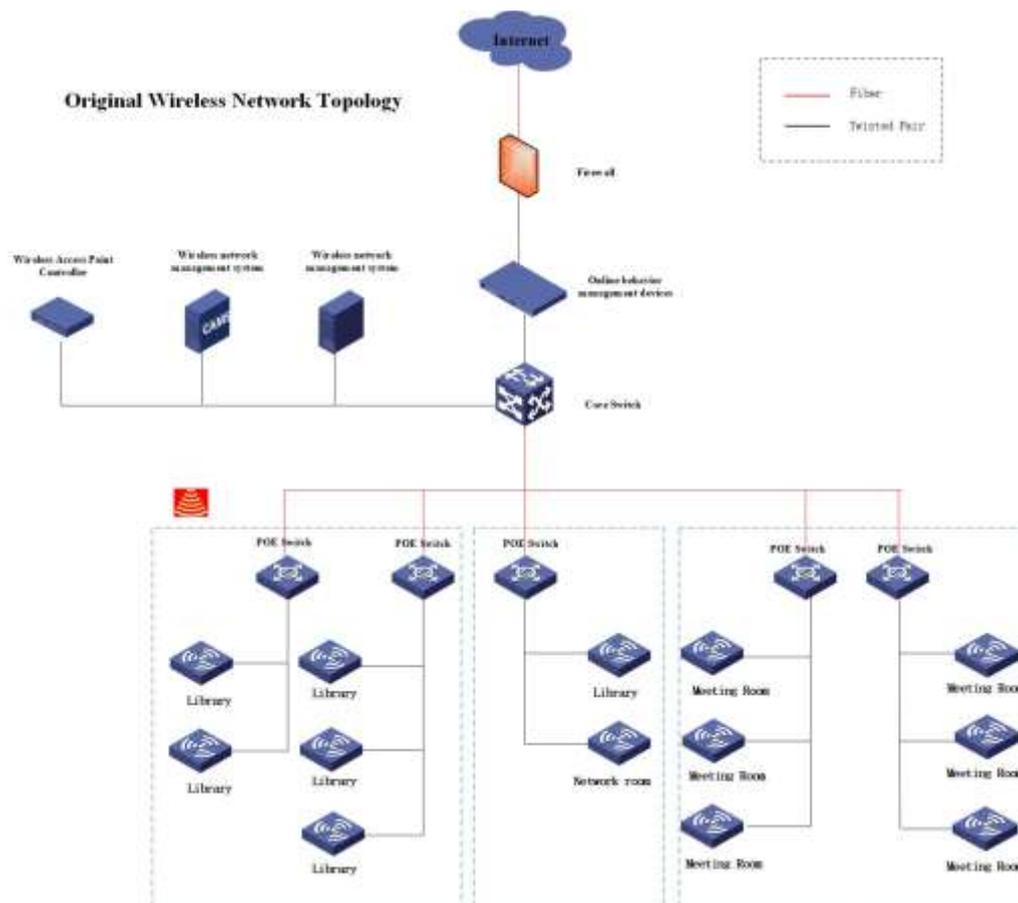


Figure 1. Original Wireless Network Topology.

In recent years, with the increasing attention to network security, the Cyber Security Law of the People's Republic of China has been issued. The law has made demands on the retention time of the internet access logs and the network address translation logs. The original wireless system can no longer meet the relevant requirements. On the other hand, with the development of technology, the wireless system using the 802.11a/b/g/n protocol is difficult to meet the user's needs in terms of

communication rate and anti-jamming, and it is difficult for WEP as an aging encryption algorithm to ensure the security of user data. Therefore, the National Engineering and Technology Library wireless system transformation work began to start. The original network structure is shown in Fig. 1; the post-implementation network topology is shown in Fig. 2.

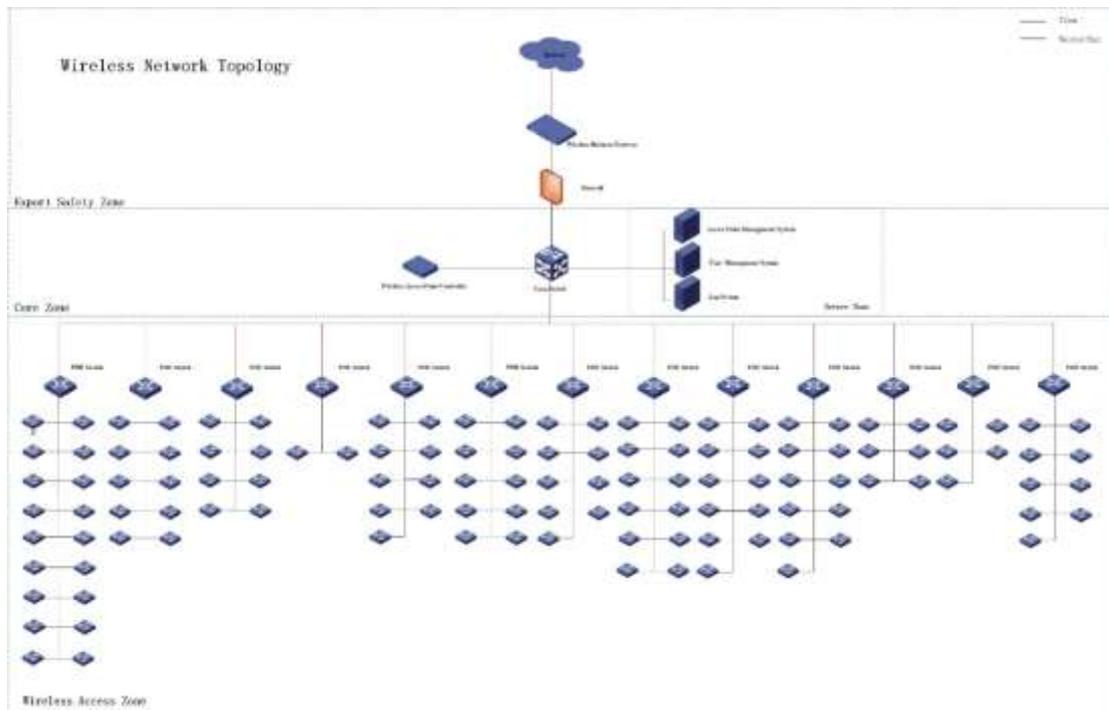


Figure 2. Wireless Network Topology.

The Development of Wireless Network Technology

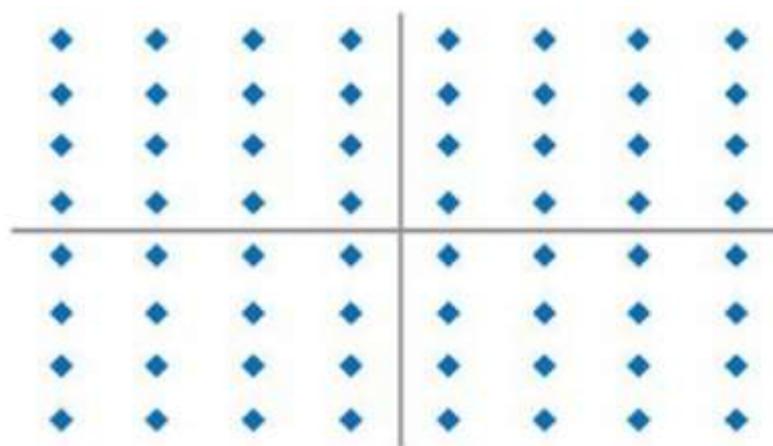


Figure 3. 64-QAM Schematic.

In the application of wireless network data transfer standards, the 802.11ac wave1 standard have been widely used, 802.11ac wave2 standard has been used on some devices. Compared with the 802.11n protocol standard used by the original engineering library wireless system, the 802.11ac protocol standard mainly introduces 256-QAM modulation mode, 80/160MHz bandwidth and MU-MIMO technology, which has a significant improvement in single link speed and bandwidth utilization. Compared to the 64-QAM modulation mode of 802.11n, the modulation mode of 256-QAM allows the wireless device to include more data .64-QAM and 256-QAM diagram is

shown in Fig.3 and Fig.4 for each signal transmission. From Fig.3 and Fig.4, it can be observed that the packet density of 256-QAM is relatively higher, although with the increase of QAM level, the error rate will also increase, but 802.11ac standard theoretical speed is still higher than 802.11n. In terms of bandwidth, 802.11ac introduced 80/160MHz, which significantly increased its theoretical rate from 600Mbps to 6933Mbps. In terms of improving the efficiency of data exchange, 802.11ac uses MU-MIMO instead of SU-MIMO mode, enabling multiple users to transmit data with wireless devices at the same time, greatly improving the wireless device's ability to handle high-density user application scenarios.

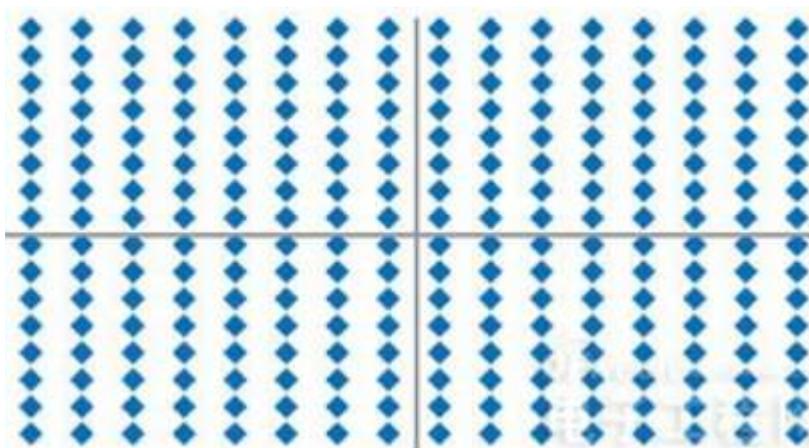


Figure 4. 256-QAM Schematic.

Technical Route for Building the National Engineering Library's Wireless Network

To strengthen the wireless network management of the National Engineering Library and realize the efficiency and standardization of the wireless network system, we must establish a hierarchical regional operation system to realize centralized management. The technical route of the National Engineering Library's wireless network is:

(1) Through the logging equipment and wireless security gateway, the network NAT logs and the internet access logscan be recorded for 200 days, which meet the requirements of the Cyber Security Law of the People's Republic of China.

(2) The wireless network is divided into wireless access zone, core area, server area and security zone. The wireless access zone mainly deploys POE switches and AP devices, the core area mainly deploys core switches and wireless controllers, the server area mainly deploys wireless business management servers, the security zone mainly deploys firewalls and wireless network security gateways.

(3) Use the core switch to achieve isolation between regions, through the ACL to prohibit ordinary wireless users access to the server area, core area and security zone, only allow administrators to initiate access to wireless network management devices.

(4) The use of wireless controller to management AP group attribution, AP signal frequency, signal transmission strength and other configuration, while AC use CAPWAP tunnel to transmission data between the user and AC, so that any user device in the wireless local area network cannot access other user devices.

(5) Use the wireless network authentication platform to achieve authorization, user account management functions. Wireless security management platform supports 802.1x, Portal, VPN and other authentication access methods, support SMS verification code/URL authentication, two-dimensional code authorization authentication, two-dimensional code business card authentication.

(6) The wireless network management platform is used to realize the functions of device configuration disaster protection, overlooking network information, and fine management of wireless network device.

(7) Through the logging device and user authentication platform seamless docking to combine user authentication online information and export logs to achieve the user online real-name information statistics. Nat logs, URL logs, BBS logs and mail logs are retained for 200 days in accordance with the Cyber Security Law of the People's Republic of China.

(8) The use of wireless network security gateway can realize the application layer filtering, anti-attack, anti-scanning, and management the Internet behavior of the internet users, blocking a variety of non-work-related websites, create a good working atmosphere, improve work efficiency.

Key Technologies of the National Engineering Library Wireless System Network

CAPWAP Tunnel Technology

First the AP zero configuration starts, and obtains the IP address through DHCP, obtains the IP address of AC, and then establishes the CAPWAP tunnel. AP can get configuration from AC via CAPWAP tunnel. Then the AP broadcasts the SSID after obtaining the configuration and converts the 802.11 data frame and the Ethernet data frame. The wireless AP access point communicates with the wireless controller in standard CAPWAP encrypted tunnel mode, ensuring the content security during data transmission.

Virtual Wireless Access Point Technology

Through the virtual wireless access point (Virtual AP) technology, the device can provide multiple SSIDs, support multiple 802.1QVLAN, network manager can use the same SSID subnet or VLAN separate encryption and isolation, and can be configured for each SSID separate authentication method, encryption mode and so on [1].

RF Detection Technology

The RF probe scanning function can detect illegal access points, or other sources of RF interference in real time, and provides alerts function which enable network operators to monitor potential threats in various wireless environments.

Wireless Controller Cluster Technology

All users' online connection information and roaming records can be synchronized in real time between multiple wireless controllers. When wireless users roam, through the sharing of information and authorization information within the AC cluster, users can cross the entire wireless network, and maintain good mobility and security, keep IP address and authentication status unchanged, so as to achieve support for fast roaming [2].

To support seamless roaming within key coverage areas, wireless systems support L2 roaming. Wireless data streams can be forwarded locally without using wireless controller. Local forwarding technology completely breaks the traffic bottleneck limit of wireless controller. According to the network's SSID and user VLAN planning, determine whether the data needs to be all forwarded through the wireless controller, or directly into the wired network for local exchange. Local forwarding technology will forward latency-sensitive and high-real-time data through the wired network, in 802.11ac environment, can greatly reduce the traffic pressure of wireless controller, better adapt to the future wireless network higher traffic transmission requirements, such as high-definition video-on-demand, VoWLAN transmission and so on.

Acknowledgment

This work was supported by a grant from Institute of Scientific and Technical Information of China. The authors would like to thank Yang Han for excellent technical support.

References

- [1] Shaoqing Wang. “The design and implementation of the university's digital campus platform based on the integrated virtualized cluster server.” Zhejiang University of Technology, 2017.
- [2] Pei Fang. “The design and realization of unified ID card under various access modes.” Yunnan University, 2011.