IDC Engine Room Tiny Sniff System

Yifan Qiang

Department of Electronic and Communication Engineering, North China Electric Power University, LianChi District, Baoding 071003, China.

qyf201809@gmail.com

Abstract

This project uses an anti-surge imitation STM32 hardware circuit with independent power supply to detect the network connection or delay status of the IDC room through the ping function, and upload the sniffing results to the independent server through the mqtt protocol for remote monitoring by the operation and maintenance personnel through the browser. It can be used for link maintenance of small, medium and large cluster servers. Moreover, it solves the problems of low maintenance efficiency and high maintenance cost of traditional personnel, improves the efficiency and availability index of IDC room operation and maintenance, reduces the incidence of failures, and ultimately improves the human and economic benefits of the enterprise and the quality of operation and maintenance services. Summarizing the project's content as the project leader is the final procedure.

Keywords

IDC Engine Room, Sniff System, Imitation STM32, MQTT, Cloud Platform.

1. Introduction

With the continuous development of network technology, the application of computer networks has become more and more extensive, and its role has become more and more important. However, due to the fragility of the software and hardware in the computer system, the fragility of the computer network and the geographical location, the natural environment, natural destruction and the influence of human factors, not only the risks of information storage and processing are increased, but also new information transmission problem. Network security problems are getting more and more serious, and the losses caused by network damage are getting bigger and bigger. Network security has become an urgent problem to be solved. The first thing most hackers do after successful intrusion and implantation of backdoors is to choose a sniffer suitable for the current network to obtain more information about the victim. Sniffer is a commonly used method of collecting useful data and can be used as a device for analyzing network data packets.

A network sniffer is a tool that uses a computer's network interface to intercept data messages from other computers, and it is different from a general keyboard capture program. The keyboard capture program captures the key value entered on the terminal, and the sniffer captures the real network message. If the network sniffer is placed at the network node, it is a passive way to capture the data frame in the network Monitoring means is a commonly used method of collecting useful data. It can analyze various information packets and describe the structure of the network and the machines used. Since it receives any data packet transmitted on the same network segment, it also exists To capture the possibility of unencrypted information such as passwords, various information, and secret documents. This has become a common method used by secret thieves to expand their results to seize control of other hosts. Of course, the legitimate use of a sniffer is mainly for network managers to analyze network traffic in order to find potential problems in the network of concern. For example, suppose that a certain segment of the network is not running very well, the sending of packets is relatively slow, and we don't know where the problem is, then we can use a sniffer to intercept the data packets in the network to analyze the problem.

In addition, the maintenance efficiency of the maintenance personnel is closely related to the overall cost of the IDC operation and maintenance company. The timely detection of link failures can also improve maintenance efficiency and reduce maintenance costs to improve economic benefits. And improve the IDC Engine room availability index, reduce the incidence of failures, improve the efficiency of operation and maintenance, timely discover and solve problems, and improve the quality of operation and maintenance services The maintenance of the network is the ultimate goal of network sniffing. The design of a single-chip microcomputer with sniffing and forwarding functions, as well as the circuit environment for machine operation, and finally the realization of the monitoring function on the visual interface is the key and difficult point. This project researches communication systems based on computer networks, involving equipment selection and PCB board selection.

2. Sniff System Introduction

2.1 System Model Diagram

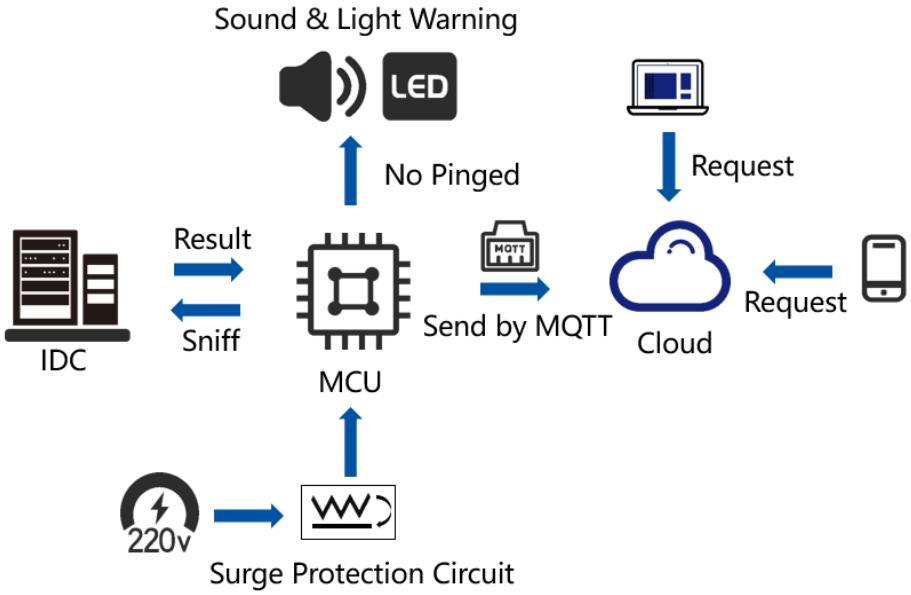

Fig. 1 System Model Diagram

2.2 Core Module & Functions

MCU: Sniffing the IDC computer link status and sending the sniffed results to the cloud platform using the mqtt protocol. Once the link fails, an audible and visual alarm will be issued locally to notify personnel of timely operation and maintenance.

Surge Protection Circuit: Preventing MCU sniffing failure caused by unstable power supply voltage in the equipment room. In this subject, an adapter is adopted to convert the 220V AC power to 5V MCU DC power.

Cloud: Accepting the mqtt data packet from the single-chip microcomputer, analyzing the data content and displaying it visually on the webpage so that mobile terminals such as mobile phones and computers can monitor the network status anytime and anywhere. In this project, group uses Alibaba Cloud services.

2.3 System Workflow

MCU uses the mqtt protocol to send data to the server located on the cloud platform through multiple channels (wireless or wired) by sniffing the network link status of the IDC room in the current network segment. The server processes and integrates the collected data, and visually displays the results on the server's webpage, so that the operation and maintenance personnel can monitor the IDC room link status anytime and anywhere with multiple terminals.

3. Team's Work

Work can be divided into three stages according to the length of the project and the inspection.

3.1 Early stage

Firstly, team learned STM32 basics and Synthesis, including LED, LCD, buzzer, button, serial communication, DM9000, network communication, Computer Network (OSI reference model and TCP/IP reference model), etc. Secondly, based on STM32, group ported the LWIP protocol to the microcontroller. Thirdly, Learn the principle of ICMP and the structure of the data message, add parameter information such as IP address and MAC address according to the message structure to form a Ping request packet, and send the data packet to the target host. According to the returned Ping response message, the link status is analyzed. Finally, Learn the principle of ICMP and the structure of the data message, add parameter information such as IP address and MAC address according to the message structure to form a Ping request packet, and send the data packet to the target host. According to the returned Ping response message, the link status is analyzed. Since then, the project function has been basically realized.

3.2 Middle stage

Since the purchased single-chip microcomputer was used in the early stage of the project, most of its functions were not used. At the same time, in order to exercise the abilities of the members, the team decided to make only the functional single-chip for the project in the mid-term. Design the 5 steps of designing, drawing, collecting, welding and verifying the components of the single-chip microcomputer. Finally, the new MCU was created.

3.3 Final Stage

At first, in the process of using Alibaba Cloud services, the team realized that the degree of customization of the project's cloud platform was not high enough and the performance was limited. So we decided to improve the cloud platform. That is, renting an independent server and learning the relevant front-end and back-end knowledge of building web pages. At the end, the performance of the cloud platform and web page has been improved.

4. Project Results

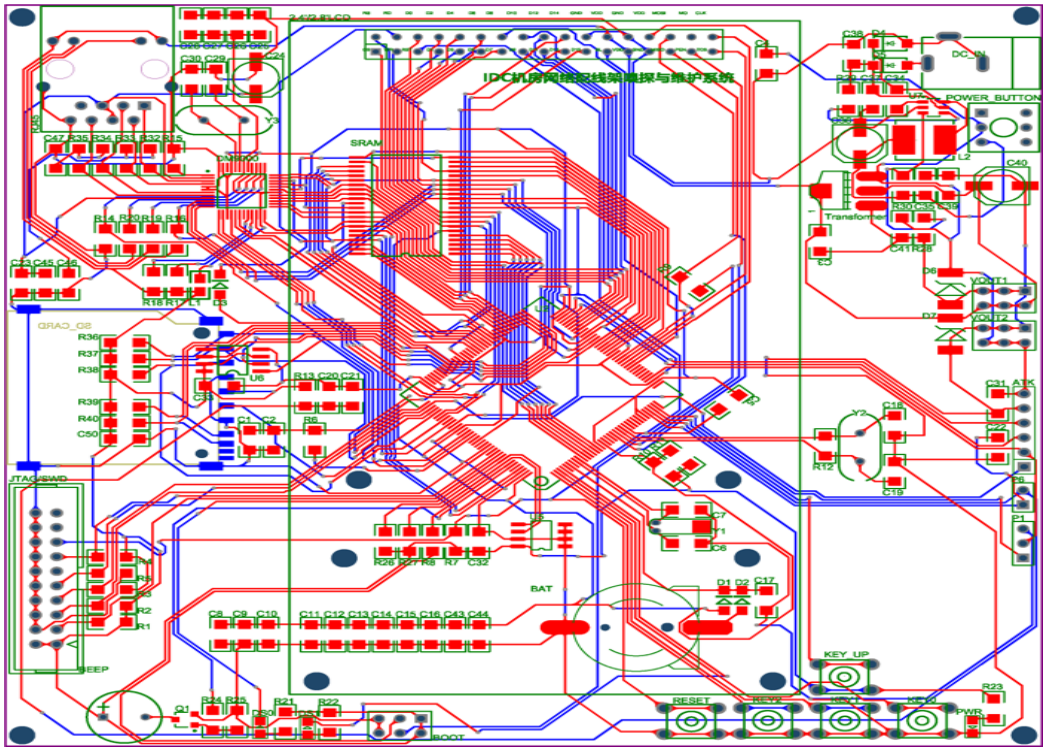

Fig. 2 PCB Trace Diagram

Project outcomes include: MCU function code and cloud platform front-end code; Plan to make a single-chip with detection function and work normally; Successfully applied for a practical and innovative patent. Picture are as follows:

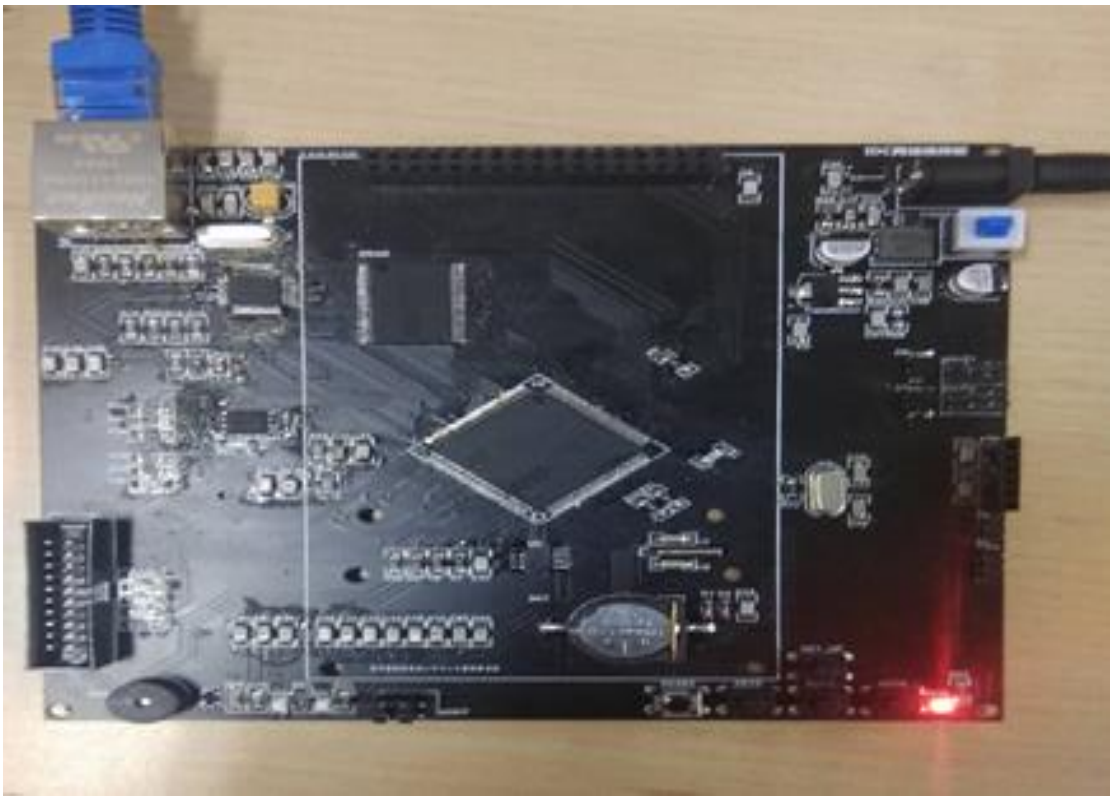

Fig. 3 SCM Board (After welding)

5. Project Innovation

Firstly**,** the hardware and software are combined to analyze the data package, B/S is to achieve the goal, and the browser side has a high degree of freedom in writing (style/function).

Secondly, secure: the collected data is stored (local/cloud), and the browser-side access page is concise and clear.

Thirdly, real-time: the sniffing result detects the connection status of the device in real time and returns it to the cloud platform monitoring system.

Finally, convenience and saving: The single-chip microcomputer is in the chassis, which does not take up additional space and is independently powered.

6. Conclusions

Project status: Has basically achieved the original goal, which are:

Developed the stm32 single-chip microcomputer that realizes the purpose detection function; wrote the html file of the browser version to analyze and sniff the data packet; design the principle of the anti-surge circuit; publish related papers or apply for related patents, technical reports.

Acknowledgments

This project was financially supported by North China Electric Power University (Baoding) fund. Besides, I would like to extend my sincere gratitude to project supervisor, Zhiqi Hu, for her instructive advice and useful suggestions on this process. I'm deeply grateful of her help in the completion of this national level project.

8. References

[1] https://www.st.com/zh/microcontrollers-microprocessors/stm32f103.html.

[2] https://savannah.nongnu.org/projects/lwip/.

[3] http://www.openedv.com/.

[4] Huoliang Liu, Seng Yang. LWIP is based on STM32 application development guide [M]. China Machine Press, 2019.

[5] Andrew S. Tanenbaum. Computer Network (Fifth Edition) [M]. Tsinghua University Press, 2012.