Realization of Instructional Network Data Analysis Instrument

Ping WANG*

Fuzhou University of International Studies and Trade, China, FuJian, Fuzhou, 350202

*Corresponding author

Keywords: Networks data, Capturing, Portable, WinpCap, Embedded.

Abstract. In order to improve the teaching quality of computer network course, with the deficiency of the current networks data analyzer, this paper puts forward a designing ideas for it, and discusses the analyzer’s designing plan. We select S3C2440 as a processor and analyze the functions of all the constituent parts based on block diagram of the system hardware structure. On realization, we adopt WinpCap as the development packet, analyze the principle of capturing networks data, show the correlative realization code. After all, we summarize the problem and its resolvent of the portable networks data analyzer.

Introduction

With the popularization of network applications, people pay more and more attention to network security and network failures. There is an urgent need for a well-functioned and easy-to-use network data analysis device or tool. Sniffer (sniffer) is widely used at present. Sniffer is a technology that uses the network interface of computers to intercept data messages from other computers. This technology is widely used in network maintenance and network management. Sniffer receives all kinds of information from all computers in the network. Through the analysis of these data, network administrators can deeply understand the current network operation status, in order to find out the potential problems in the network [1]. The inconvenience of this powerful tool in use is that it must run on the PC platform, and it is difficult to achieve portability and mobility.

The emergence of WinpCap greatly facilitates and simplifies the development process of network data capture program. Literature [2] - [8] has related expatiations in this respect, and put forward some ideas with reference significance. However, it is not difficult to find that some of the documents are mainly introduced in theory, and there is no relevant practice development process. Secondly, for the documents that give the development process, they are all based on PC platform applications. We suggest that this can directly use existing software such as Sniffer, which is widely used at home and abroad, without self-development, so from the application point of view, based on PC platform. Development doesn't make much sense.

Referring to some existing theoretical results, the purpose of this research is to develop an application program with Sniffer function on the embedded platform to capture and analyze network data. As a portable network data analyzer, it replaces the working mode of PC + application software, assists and cooperates with PC when it is difficult or impossible to use, and makes network maintenance and management more convenient.

System Design

The design of portable network data analyzer is divided into two parts: hardware and software. The 16/32 bit processor S3C2440 with ARM920T core is selected as the hardware part. S3C2440 is an embedded microprocessor developed by Samsung Corporation of Korea, which can be used to develop portable products such as handheld devices and smart home appliances. Its main frequency processing speed can reach 533 MHz. It has the characteristics of high cost performance and low power consumption. The functions integrated on the chip include SDRAM controller, NAND Flash
controller, LCD controller, touch screen and other interfaces, which greatly simplifies the design of peripheral circuits.

**System Hardware Design**

The hardware design of the system consists of the following parts:

- **Processor**: Samsung S3C2440A, ARM920T core, main frequency 400MHz;
- **64M Bytes SDRAM**, using two Samsung K4S561632H-UC75 chips;
- **64M Bytes Nand Flash**, using Samsung K9F1208UOB chip;
- **A 100Mbps Ethernet interface**, using RTL8019AS chip;
- **SHARP 3.5'TFT LCD** (with touch screen);
- **Keyboard matrix**.

The system structure block diagram is shown in Figure 1.

![Figure 1. The system structure block diagram.](image)

- **64M SDRAM** is the storage space used by the operating system when it runs;
- **64M Nand Flash** is used to store the kernel image files and user data of the operating system;
- **The network module** realizes the network access function of the system, which is also the key to the realization of the system function;
- **LCD** (with touch screen) and keyboard matrix are used to achieve good human-computer interaction;
- **The power management module** provides a variety of voltages needed by the system - 1.8V for the chip core, 3.3V for the chip I/O port and 5V for the off-chip conventional integrated circuits. The power management module solves the power supply requirements of all parts of the system, reduces the power consumption, reduces the interference noise between different power supplies, and improves the integration of the system.

**Acquisition Principle of Network Data**

The capture of network data can be achieved in two ways: one is by utilizing the broadcasting characteristics of ethernet, the other is by setting the monitoring ports of network devices. Data transmission in Ethernet has broadcasting characteristics, and all network ports in LAN have the ability to access all data transmitted on physical media. But generally, after the network card receives a data frame from the network, it needs to check the address matching first. Only the data frame matching the MAC address of the network card or the broadcast address or the specific multicast address is submitted to the operating system kernel, and all other data frames are discarded. The application program only receives the data arriving at the local computer. In order to capture data flowing through the network card but not belonging to the local computer, the working mode of the network card must be set to promiscuous mode. When the network card works in this mode, it has the ability to receive all the data arrived at the network card. It interrupts all the received data frames, does not match the address, and directly submits all data frames to the system for processing. By directly accessing the data link, the operating system can capture all the data messages flowing through the network card. Setting a network card in hybrid mode requires the support of the network card driver. The driver sets the network card in hybrid mode through system I/O calls, thus skipping the address matching check $^6$.
Development Points Based on WinpCap

Winpcap is a free and public network access system under Windows platform. It provides Windows 32 applications with the ability to access the bottom of the network. Winpcap can't block, filter or control the sending of other application datagrams. It just listens to the data transmission on the shared network. Winpcap is composed of three modules: the kernel-level Network Packet Filter (NPF), the user-level dynamic link library Packet.dll and Wpcap.dll.

Because this system is based on embedded platform and uses Windows CE as the operating system, Winpcap for Windows NT4/2000/XP/2003/Vista, which has been tested and applied, can not be directly used in this system. Winpcap for winCE driver download is available on Winpcap's official website. Source code is provided, but it was tested on pocket PC of ARM chip of hp, and the version of Windows CE used is less than 4.2. Therefore, it must be modified to use under Windows CE 4.2. The general modifications are as follows:

a. NDIS version, the original version number is 2, while the middle driver version number on Windows C 4.2 should be set to 3;

b. It searches the network card by searching the corresponding key value in the registry. It must know the key value in the registry corresponding to the actual available network card;

c. There are two parts in the source code. One is the pktDrv project (generating pktDrv.dll), which is a dynamic link library driven by the middle layer, and the other is the Winpcap function implementation based on it (this does not need to be changed at all). How to use it can refer to a test program provided in the source code (download address: http://www.winpcap.org/install/default.htm, compression). The test program can then be found in the folder SampleApp.

The development process of data capture is mainly based on Figure 2.

Some of the main implementation codes are as follows:
Char * dev = pcap_lookupdev (char * errbuf); // Select network interface
Pcap_t*adhangle = pcap_open (dev,//open device) 65536, // Set the captured data length to a maximum of 65536.
PCAP_OPENFLAG_PROMISCUOUS, // Set to Hybrid Mode
1000, // Set 1S timeout
NULL, errbuf);
Pcap_compile (adhangle, & fcode, packet_filter, 1, netmask);//compile filtering rules
// Where packet_filter is an array that defines filtering rules for receiving user settings
Pcap_setfilter (adhangle, & fcode);//Set filter rules
Pcap_loop (adhangle, 0, packet_handler, NULL); //Cyclic capture of network data

![Figure 2. The development process of data capture.](image-url)
Conclusions

This paper presents a design idea of portable network data analyzer and builds a platform to implement it. Practice has proved that the system design is feasible in implementation, and can complete the capture and analysis of common data packets in network maintenance and management. However, there are still several problems to be further improved or solved:

a. Perfection of function. The functions provided by Winpcap are limited, especially for the acquisition and analysis of the underlying network data, which need to be further improved. Secondly, we should integrate as many network protocols as possible to make the functions more perfect. Moreover, good user interface and human-computer interaction are another important aspects to be considered on the basis of realizing the proper functions.

b. Network access. For local area networks, network access is not involved. But when it is necessary to apply the system to the Internet, Network access function has become the primary consideration. Nowadays, there are many kinds of network access authentication systems, such as the interconnected satellite sky of telecommunications, CNCMA of Netcom - "Broadband My World" and Ruijie Security Authentication Platform, which provide client authentication software for users, but these software are all based on PC. Porting it directly to embedded system will become an invalid application. Therefore, in order to realize the network access of the embedded system, we must develop the authentication software suitable for the embedded system according to the authentication mechanism of various networks.

References


