The Design and Implementation of Network Monitoring and Analyzing System Based On Campus Network in Higher Vocational Colleges

Li Xinxia[1,a]

[1]Department of engineering and technology, Shandong Vocational College of Foreign Affairs Translation,Weihai,264504,China

[a]email:wsfylee@163.com

Keywords：Higher vocational education; Campus network; Traffic monitoring analysis; Winpcap technology

Abstract. With deepening the construction of modern vocational education system, how to develop vocational education has become a major hot issues in education in China. Studying the characteristics of vocational education students is to be one of the precondition of how to develop vocational education. This paper designs a network monitoring and analyzing system based on the higher vocational colleges by studying the characteristics of vocational students to obtain first-hand technical information. The system uses Winpcap technology implementation of campus network traffic statistics, data acquisition, protocol analysis, etc.

Introduction

Higher vocational education in China after more than ten years of development, has switched from scale expansion to the substantial development of the stage. The Ministry of Education has launched a series of policies and promoted the development of higher vocational education. “National medium and long-term education reform and development plan outline (2010-2020)”explicitly pointed out that we should vigorously develop vocational education, improve the quality as the key point. How to improve the quality of vocational education has become the major hot issues in education in China. Familiar with the characteristics of the object of education is the necessary premise to better improve the quality of education, and putting forward with the project was based on this purpose

This paper based on campus network in higher vocational colleges, from the perspective of the research network application, a network monitoring and analyzing system is designed. The system is mainly to solve the following problems: 1. Campus network quantity monitoring. Though master the campus network using regularity to facilitate planning and construction of the campus network. 2. The campus network protocol analysis. It’s to master the campus networking protocol distribution.3. Network anomaly traffic monitoring, is to discover the network anomaly traffic and illegal access and to determine the specific location.4. Database management based on Web, the system management can inquire related data at any campus network terminal.5. The construction of campus network. The data will be further analyzed to understand network users’ demand and targeted to enrich the contents of the campus network, better giving play to the role of campus network publicity, and guiding, creating a good campus culture atmosphere.

System Function Description

The system user defined: This system user is defined as the campus network monitoring and maintenance department and the construction of campus web department related personnel.

The system has the network traffic collection function: All packets are caught and analyzed in the campus network. The source/destination MAC address, source/destination IP address, port number, protocol type, packet size, receiving time and other information of the package are stored to the database.

Network flow statistics and analysis function: the collected information will be statistics and

analysis, then in the form of graphics display under different time granularity distribution of network traffic and protocol.

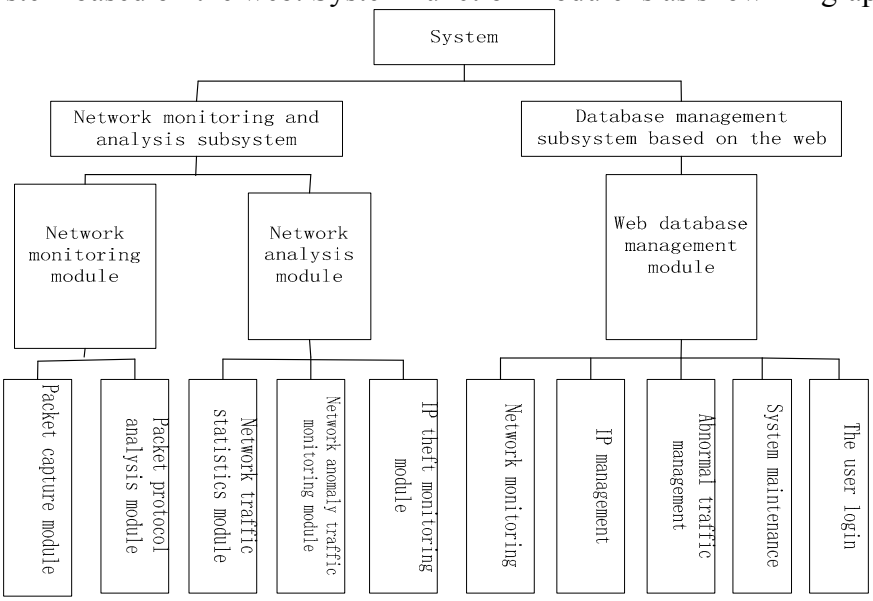
IP address management functions: the users of the campus network are assigned only IP address, through the IP - MAC address binding method to prevent modify the IP address. Once appearing afore-mentioned problems system automatic alarm and showing the location of the computer, store the alarm records in the database for the management staff query.

Network anomaly detection capabilities: system through the threshold detection method, anomaly traffic detection model is established. When abnormal network flow, system will notify the network administrators and take measures to deal with abnormal situation, at the same time the abnormal situation will be stored into the database.

The database management functions based on the web: According to different user access, users can log in network terminal to query network real-time traffic, traffic history and protocol distribution. Administrator can also realize the system maintenance operations such as IP, MAC address binding, etc.

The System Function Design

The whole system consists of two parts: network monitoring and analysis subsystem ,database management subsystem based on the web. System function module is as shown in graph1.



Graph1 System modules

System Implementation

1.The realization of network monitoring module

This module contains the packet capture and protocol analysis. College campus network uses the bus Ethernet structure. Using the characteristics of bus Ethernet nic is set to promiscuous mode, realizing and capturing the transmission of all packets in the network. Capturing packets are stored into the user buffer, and for every physical frame add Winpcap head and populate the fields, the unit composition of new data is stored in the structure of the LPPACKET Buffer area.

Packet protocol analysis procedure is described below:

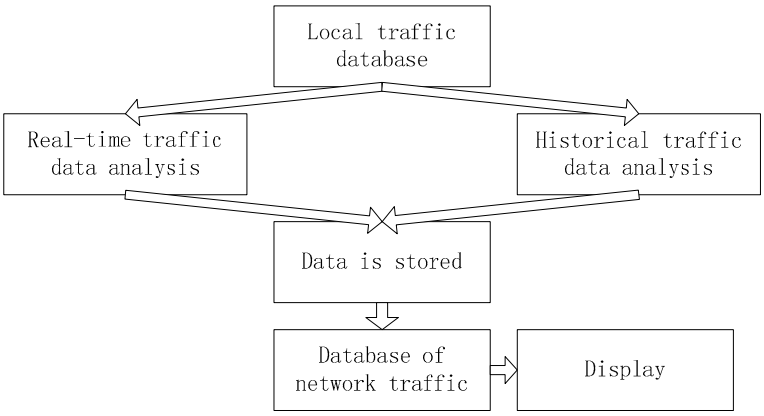
```
struct bpf_hdr *hdr;
int offset=0;
buf=(char *)Recvpacket->Buffer;
BytesReceived=Recvpacket->ulBytesReceived;
 While（offset< BytesReceived）
{
   hdr=( struct bpf_hdr *)(buf+offset);
   tlen=hdr->bh_caplen;
   offset=offset+hdr->bh_hdrlen
   packet=(char *)(buf+offset);
   pEtherHead=(struct ethernet_head *) packet;
   smac=&( pEtherHead->ether_shost);
   dmac=&( pEtherHead->ether_dhost);
   switch(swaps(pEtherHead->ether_type));
{
    case ETHER_PROTO_IP;
     pIPHead=(struct IP_head *)(packet+ETHER_HEAD_LEN);
     iIphlen=sizeof(unsigned long *)(pIPHead-> ip_vhl& 0xf);
     sip=&( pIPHead->saddr);
     dip=&( pIPHead->daddr);
     switch(pIPHead->ip_proto)
      {
        case IP_PROTO_TCP:
          DecodeTcpPack(packet+ETHER_HEAD_LEN+iIphlen);
        Break;
        case IP_PROTO_UDP;
          DecodeUdpPack(packet+ETHER_HEAD_LEN+iIphlen);
        Break;
……
}
          case ETHER_PROTO_ARP;
                ……
          case ETHER_PROTO_RARP;
                ……
           }
          offset=Packet_WORDALIGN(offset+tlen);
}
```

2. The realization of network analysis module

This module is the core of the system. It is composed by the network traffic statistics module, network anomaly traffic monitoring module and IP theft monitoring module.

(1) Network traffic statistics module

Involves a lot of database interactions in the module, there are four main function modules. Function module as shown in graph2.



Graph2 Network traffic statistics module function module graph

Data real-time processing and analysis function is based on the data acquisition to analyze and do statistics of the real-time traffic. Statistical information is contained: The network traffic load, distribution network protocol, and packet size distribution. This work is finished in three steps: First of all, through real-time traffic statistics function, this will separate the traffic information in the packet protocol analysis module. Then create temporary table store isolated traffic information. Finally call the SAVE function to store the information in the temporary table, and through SaveToDatabase function to store real-time traffic information in web database.

Historical traffic data analysis is calculated by time unit respectively such as hour, day, and month .The procedure is described below:

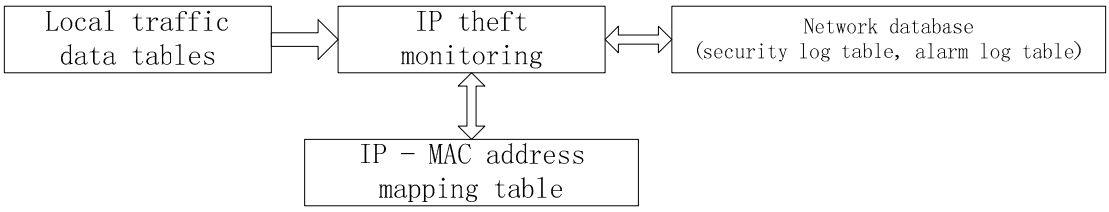
To set the original packet capture time sequence t1，t2，……，tn，to set attribute values for each time sequence n1，n2，……，ni。

```
int i=1,T0=ti;
while((ti+△ T)>ti+1)
{
      total=0,n=ni;
      while（（T0+△ t）≥ti+1）
         {
           if（n<ni+1）n=ni+1
           total=total+ni*(ti+1-ti) ;
           i=i+1 ;
}
total=total+ni*(T0+△ t-ti) ;
n̄=total/△ t;
Save(T0,n, n̄);
};
T0=T0+△ t ;
}
```

(2) IP theft monitoring module

In this system, each computer is distributed to fixed IP address, the IP address theft monitoring is accomplished by means of a MAC address binding IP address.

Running under Windows NetBios protocol encapsulation command NBTSTAT to obtain host MAC address and then establish IP&MAC address mapping table. Comparing traffic information of IP with MAC address in local traffic data table storage with IP - MAC address mapping table, the result doesn't conform to alarm and record the information into the alarm log tables and security log tables. The principle is shown in graph3.



Graph3 IP address monitoring principle diagram

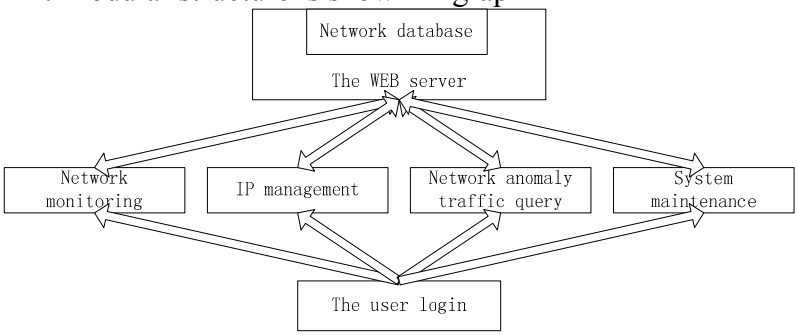
(3) Network anomaly traffic detection module

The module adopts the method of threshold monitoring detection of abnormal traffic. According to the network traffic for a period of time monitoring and statistics get the flow indicators. Through calculating parameter variance, set a normal parameter confidence interval. Comparing real-time traffic with the area, it goes beyond the normal range and indicates that traffic may be abnormal.

When abnormal flow, this system adopts the play wav files in the VC to give an alarm, and notifies the administrator for processing.

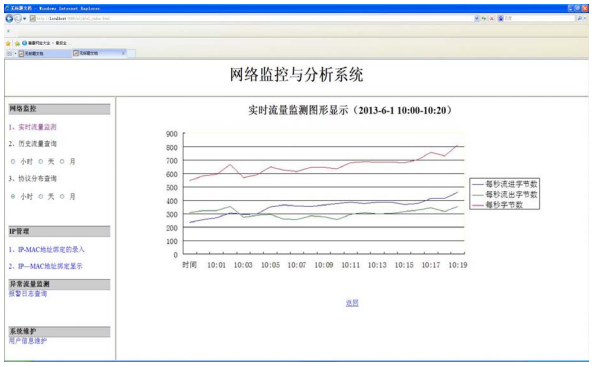
3. The realization of Web database management module

This module uses the ASP technology to realize network database query maintenance, and other functions based on WEB. Modular structure is shown in graph4



Graph4 Web database management module

System main interface screenshots are shown in graph5 and graph6.



Graph5 Network monitoring module real-time traffic query graphical display interface

Graph6 protocol distributed query graphical display interface by the hour

The Results Analysis

Through the deployment of the system test, analyzing the network traffic has the following features about our campus network.

1. Network traffic's direction is in accordance with the school hours. Working day network traffic peak appeared after 5 p.m. Every Tuesday and Thursday was the peak of the traffic flow, less on Monday and Friday.

2. Through the network traffic monitored 24 hours a day, this found that the uplink bandwidth is large, on average in 50 M or so, the highest peak is 100M. Uplink bandwidth repression increased downlink bandwidth rate, prevent the jam. Through the analysis of protocol traffic trends, its hairy

peak is more, not suppressed and more use of bandwidth, peak value of the total bandwidth is in the ideal range.

3. P2P application takes up a lot of bandwidth. From the test results, the P2P traffic has exceeded the total of the conventional protocol network traffic, mainly P2P applications focused on various applications such as thunderbolt, BT download.

4. Network security problem doesn't allow ignoring. According to statistics, a day of network attack an average of 268 times, the threats are security to network.

5. Analysis from the aspects of network application. The Internet has become an indispensable part of students' daily life, and become a main medium for the students to understand and communicate with the outside world. By analyzing the captured packets , we found that main network applications focused on data download ,information query, browse news, communication, blogs, micro blogging distribution, network virtual games, video browsing, shopping, online books, etc.

Reference

[1] W．Richard Stevens TCP／IP IllustratedVolume1：The Protocols Chino Machine Press. 2000:4

[2]Xu Xiayi. A network traffic check and analysis system based on windows operating system according to national tax [D].2004:4

[3] Towards a systemic understanding of the Internet organism：a framework for the creadon of a Network Analysis Infiastructure http：//moat．nlam'．net/NAF 1998

[4] DLPI STREAMS Driverhttp://publib．boulder．mm．com/doc_link/Zh_TW/a_．doc_lib/libs/commtrf2/dlpi．html

[5] W．Ricbard Stevens TCP/IP IllustratedVolume 2：The Implementation. Chino Machine Press 2000:4

[6] Luis Martin Garcia Programming with Libpcap--Sniffing the Network[Z]

[7] Lawrence Berkeley National Labs ． Libpcap ， Network Research Group [EB/OL]．http://www.tcpdump.org，2009

[8] Marina Fomenkov, Ken Keys, David Moore, and kclaffy Long gitudinal study of Internet traffic in 1998- 2003