The study and design on the campus network surveillance

Xu Bing*, Yizhi Zhang

Chongqing Three Gorges University, Wanzhou Chongqing, China

Received 1 August 2014, www.cmnt.lv

Abstract

In order of improving the efficiency of network administration, one of the most useful methods is to inspect and measure of the network traffic. By introducing technology relevant to network flow monitor and analysing monitor system of campus network flow, this paper brings forth collection of Campus network flow and statistic of network flow, adopting Visual C++ 6.0 technology to design structure of this plan. This paper also points the key technology and means to realize monitor system of campus network flow and monitor system of campus network flow. It is reliable and extensible to for realization of system to improve administrative function. It is easy to realize the function of collection of campus network flow and flow statistic.

Keywords: network monitor, network flow, collection of flow, data statistic, VC++ 6.0

1 Introduction

With the rapid development and wide application of computer network, network has been interfered into various fields of social life. Similarly, as an important infrastructure establishment so as to innovate education in high colleges, improve managing level and educational quality, campus area network has been elevated correspondingly. However, the secure problems consisted in its operation and management has become prominent. Therefore how to establish sophisticated secure system of campus area network has become a crucial problem to be faced and tacked by network managers.

Network will determine our life style; the quality of network will have direct influence on various respects of social and economic life. With the increase of users' demand on network property, stable operation and efficient development of network cannot be guaranteed without efficient managing system and network system. With the rapid development of infrastructure technology of constructive network and network application and increase of demand on network property, network management has become an issue to be solved immediately. Efficient network management can guarantee stable operation and lasting development of network. What is more important, due to enlargement of network scale and development of hacker technology, the number of cases about invasion and attack become large, which takes challenge to stable network service and information security and internet rule, so internet security has become an important role in the whole system of internet management. At present, P2P, mainstream media and network game and some new application has occupied above 60 percent of network flow [1], and hostile attack on network has become more and more. Thus identification of network flow is quite important, which is helpful for network manager to timing supervise and manage various business flows and for supplier of network service to understand condition of each business flow of network when lay outing and constructing and for internet researchers to understand character of each flow of network and correspondent users' action. Therefore supervision on network flow has attached wider attention from academic and applicative fields.

2 Adopting relevant technology

2.1 NETFLOW

NETFOLW is a network exchanging technology stipulated by CISCO Company [2], which classify and handle network flow by concept of data flow. The definition of data flow given by NETFPLOW is consisted with seven key words marked by one- way network data assemblage of two communication terminals. The seven keywords are original IP, target IP, original terminal, target terminal, negotiation type, service type and interface search. In the case of traditional network interchange, each input subgroup is handled separately, then router will take series of independent consultation for each subgroup and check visiting list, obtain charging data and exchange subgroup by resort of series of functions, after that send {exchange}it to destination. These checks include whether to adopt secure visit to infiltrate and renewing network charging record. On contrary, in terms of NETFLOW exchange, in the process of consultation, it only works on the first subgroup of the first data flow. When a data flow is identified and determined its relevant service, the later subgroups will be treated as a part of this data flow and handle it on the base of linkage. In this case, it can avoid check on visiting list and can exchange subgroups in turn.

* ***Corresponding author*** e-mail:xb_2316@163.com

Besides exchange of data, important applications of NETFLOW are count information of data flow and supervise network flow. The information of data flow counted by NETFLOW is sent to address of preset information collector in the form of UDP data packet. Information collector will receive NETFLOW data packet constantly, then analyze various flow information.

The applicative model of NETFLOW (illustrated by Figure 1), NETFLOW exchange or route equipment analyze and count flow, then send information to information collector. NETFLOW information of various information collectors will be assembled to NETFLOW SERVER, after that it will handle flow information in accordance with need of application.

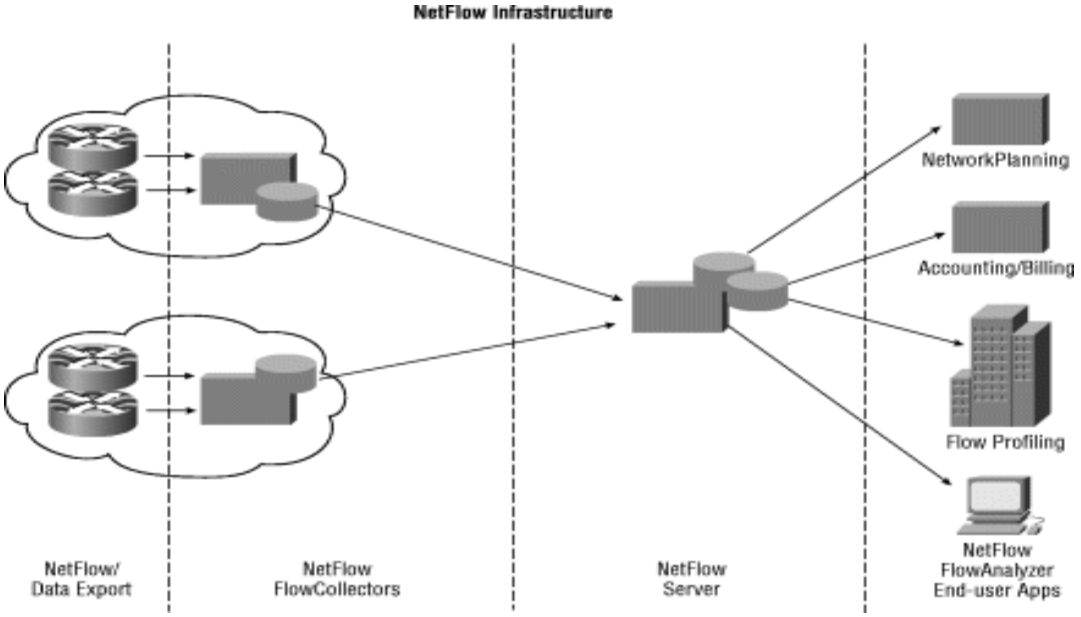

FIGURE 1 Netflow application structure diagram

2.2 PROGRAMMING INTERFACE OF TRANSPORT LAYER (WINDOWS SOCKET PROGRAMMING TECHNOLOGY)

2.2.1 The concept of Window socket

Window socket - SOCKET, as a foundation of network communication, which is suit of standard API supporting network negotiation data communication for exploration of Windows system. That is TCP/IP network programming interface. In 1994 after set as network programming standard, it experienced Winsock 1.1 and Winsock 2.0, with the final aim to adapt to the demand of explorer of applicative programmer and network servicer, and the process of communication is completed by socket communication domain. Socket is charge of input and output of data in transport layer and network layer so that shield data link layer and physic layer.

2.2.2 Type of socket

According to the nature of communication, the socket can be divided into stream socket and data gram socket. Their differences mainly are that stream socket offers bidirectional, regular, unrepeated data flow service. By contrast with data gram socket, the expense of its system is high. Data gram socket also supports bidirectional data flow ignoring reliability of transportation, unrepeated and regulation. However, it retains record delimitation. Owing to high efficient transportation of data gram, it is still used widely.

2.2.3 Sequence of byte, block and unblock

In terms of sequence of byte, different computer will adopt their own sequence to deposit data, thus when these data are used to communicated, sequence of byte need to be transferred. IP addresses and terminal numbers of network sockets functions should be arranged according to network sequence constructed by sockaddr_in. To be more cautious, before applicative procedure constructs applicative procedure, users need to transfer system- unit series number to network sequence (use htons function, on the contrary ntohs function).

Block and unblock, socket possesses synchronization block and a synchronization; in the case of block model, socket only to be finished when operation is accomplished; when socket are in unblock model, socket is marked by whether new data is up to block. Block model socket is simple, convenient, but is inefficient, by contrast, unblock model is complicated by efficient. To be mentioned, Winsock provides several I/O model to solve a synchronization issue, such as “selection”, “overlap”, “event selection”, “async selection” and so on.

3 Designing goal

Supervision of network flow and analysis tool mainly aims to timing collect network data constantly and do statistic

to obtain nature index of main opponents. Combined with theory of network flow, we can observe network situation by counted nature index and analyse changing tendency of network and find factors affecting network nature. It will realize following functions:

1) Adopting Winsock to compile original socket, socket- Raw collects data packet.

2) Analysing obtained data packets

3) Visiting parameter interface of network nature offered by operative system, obtaining total amount of flow of network card, input flow and output flow;

4) System will provide various ways to show result, such as curve graph, list and so on; it mainly adopt curve to show.

5) Adopting IP to help API obtain statistic information of network.

6) Realizing part of common alarms to continue exploring function of alarm.

4 Realization of system of network flow supervision

4.1 REALIZATION OF OBTAINING ORIGINAL DATA PACKETS

Obtaining system of data packet in network mainly relies on operative system; there are different realizing ways in different operative systems. In Window environment, we can realize the obtaining function of network data packet by network driver interface specification (NDIS), SOCK-RAW of WinSock or driving technology of virtual equipment and so on.

According to above account, original socket can avoid functions suffered by Socket, use and explore bottom negotiation, and generate needed data sheet in accordance with their own desire. I start to introduce some technical knowledge relevant to exploring catch data packet by use of original socket.

4.1.1 Before using socket, we need to understand working principle of receiving data of network card

In normal condition, network interface only correspond two kinds of data frame, one kind is just match their hardware, the other one is applied to all computer broadcast. In system, the send and reception of data frame is completed by network card. Network procedure receives data packet sent by network, and judges whether to match with hardware by hardware address. If it works, it will take notice CPU to stop to respond, then it calls network card set by driver procedure to stop procedure address to call driver procedure to receive data, after all put it into stack to do systematic handle, if not, this data packet will be discarded directly.

In the case of network interface, it possesses four receiving models of data that are broadcast, multicast, and direct and mix. Only when we set interface as mixed model, network interface can receive all data, ignoring whether addresses match, thus only we set mixed model when designing, and we can realize collection of data.

4.1.2 Working procedure and usage of socket

Generally speaking, exploring network procedure by adopting socket will be experienced by following steps: start, establishment, binding, monitor (receiving connection), connection, sending/receiving data, and close, unload and so on.

4.1.3 Designing how to obtain network data by means of original socket in windows

1) Starting socket;
2) Establishing a original socket;
3) Binding socket to local address
4) Setting operative parameter
5) Setting network interface as mixed model
6) Starting monitoring thread to receiving data
7) Quitting and closing socket.

4.2 KEY FUNCTIONS OBTAINED BY ORIGINAL DATA PACKET

4.2.1 Start function WSAS startup

int PASCAL FAR WSAStartup (DWORD wVersionRequested, LPWSADATA lpWSAData).

Each socket applicative procedure must do series of initialization work by calling this function, and this socket only can be used when call is accomplished and returned. Parameter wVersionRequested among them is the version number, high byte is the minor version, low byte is the major version, and parameter lpWSAData is the guiding principle of WSADATA structure.

4.2.2 Socket establishes function socket

SOCKET socket (int af, int type, int protocol).

All communications must be established on starting up a socket, the function of socket function is establishing socket, parameter af among them refers to address family. When socket established based on UDP or TCP, we need set af as AF_ INET and adopt IP negotiation. Function type is one type of negotiation socket. When we adopt stream socket, we use SOCK_ STREAM. When we adopt data gram socket, we use SOCK_DGRAM. When adopting original socket, we use SOCK_ RAW. Function protocol can set as 0 in the situation of default.

4.2.3 binding function bind

int bind (SOCKET s, struct sockaddr_in name, int namelen).*

The next step is bind local network interface with socket after establishing socket, function s is the established socket, parameter name is the guide of information structure of communicative object needed to be bound, namelen is the length of this structure. We should pay more attention to structure of sockaddr_in:

```
struct sockaddr_in{
short sin_family;    / address family, set as AF_INET
unsigned short  sin_port;      //pointed terminal number
struct in_addr   sin_addr;     //IPaddress
```

char sin_zero
};[8].

Due to relationship between System- unit serial number and network number, in the procedure we need to use htons and some functions to transfer.

4.2.4 Setting function WSAIoctl of interface model

int WSAAPI WSAIoctl(SOCKET s, DWORD dwIoControlCode, LPVOID lpvInBuffer, DWORD cbInBuffer, LPVOID lpvOutBuffer, DWORD cbOutBuffer, LPDWORD lpcbBytesReturned, LPWSAOVERLAPPED lpOverlapped, LPWSAOVERLAPPED_COMPLETION_ROUTINE lpCompletionRoutine).

s is a handle of socket, dwIoControlCode is the code of operative control, lpvInBuffer is the address of input block, cbInBuffer is the size of input block, lpvOutBufferis the address of output block, cbOutBuffer is the size of output block, lpcbBytesReturned is the address of the number of practical output byte, lpOverlapped is the address of structure of WSAOVERLAPPED, lpCompletionRoutine is a called routine guide after finishing guiding operation.

After finishing call, WSAIoctl return to 0, or will return to INVALID_SOCKET, applicative procedure can obtain wrong code by WSAGetLastError [5]

4.2.5 Recv

int recv (SOCKET s, char buf, int len, int flags);*

4.3 DATA STATISTIC

By use of API function in IP assistant of software, network manager can, to some extent, find bottom neck of network nature by statistic data. Main relevant functions are:

GetUdpStatistic, GetTcpStatistic, GetIcmpStatistic, GetIStatistic, we should pay more attention to IPHelpapi.lib needed to load in the project. The result of function calling can show directly by list that network managers can supervise network nature by observing change of statistic, the design of statistic interface is following.

5 Conclusions

On the basis of network flow supervision system, this essay introduces in detail main technology of network flow supervision, collection of campus network flow and statistic of network flow. This system can improve reliability and flexibility of flow supervision by measure of VC++ 6.0. In the light of operation test of campus network shows that system works stably to basically satisfy designing requirement, setting foundation of research and realization of exploring further campus network flow supervision system.

Acknowledgment

It is a project supported by the scientific fund assistance project from Chongqing Education Committee (NO: KJ1401027).

References

[1] Sen S, Wang J 2002 Analyzing P2P traffic across large networks *Proceedings of the Second SIGCOMM Internet Measurement Workshop (IMW2002)* Marseille France
[2] White Paper NetFlow Services and Applications http://www.cisco.com
[3] Liang W, Li H 2008 Research on Ways of Identifying Network Flow *Communication Technology* **41**(11) 88-90 *(in Chinese)*
[4] Yao Q, Ma H, Zhang G 2006 Flow Forecast based on self-adaptation a network managing software *Computer Measure and Control* **14**(1) 45-6
[5] Li F, Li A, Wu C 2008 Application of Advanced Arithmetic of Network to Supervision of Ultrasonic flow *Computer Measure and Control* **16**(2) 163-5
[6] Zhao G, Ji C, Xu C 2010 Research on Identified Technology of Internet Flow *Microsoft Computer system* **31**(8) 1514-20 *(in Chinese)*

Authors

Xu Bing, born in February, 1976, Chongqing, China

Current position, grades: School of Computer Science and Engineering, Associate professor and master supervisor in Chongqing Three Gorges University.
University studies: Computer Science and Engineering in Chongqing University.
Publications: 5 patents, 45 papers.
Scientific interests: computer networks and applications.

Yizhi Zhang, born in March, 1963, Dazhou, Sichuan, China

Current position, grades: Network information Center. Professor and master supervisor in Chongqing Three Gorges University.
University studies: Computer Science and Engineering in Zhejiang University.
Publications: 5 patents, 23 papers
Scientific interests: computer networks and applications.