Reformation and Considerations on the Course of Computer Network

Yungang Wei
College of Information Science and Technology
Beijing normal University
Beijing, China
toweiyg@bnu.edu.cn

Jie Lin
School of Information and Electric Engineering
China Agriculture University
Beijing, China
lj610402@sina.com

Pengfei Tang
College of Information Science and Technology
Beijing normal University
Beijing, China
201322210060@mail.bnu.edu.cn

Xiaoming Zhu*
College of Information Science and Technology
Beijing normal University
Beijing, China
zhuxm@bnu.edu.cn

***Abstract*—The paper introduce in teaching of the course of computer network, in aspects of network construction, network agreement, as well as all service acts, how to utilize the sniffers' scratch IP pack process, through their analysis, to understand every internet protocol construction. The aim of the treatments concludes in change of teaching the dull theoretical contents to be an interesting experiment and so to initialize the enthusiasm of students' learning.**

Keywords—computer network; network agreement; the sniffers; network construction

I. PROBLEM DESCRIPTION

As the boost of internet technique and its application, in recent, the most of college PC department and non-PC department, have their computer network course, and also the network experiment. In the market, you may find a variety of textbooks alike, but enabling combines the theory and the practice is still seldom. Most of them are good at theory statement, for example, in aspects of teaching internet protocol, it is usually focused in theory details, but not in fundamental internet protocol construction, or the agreement conceiving procedure[1]. The author considered that the internet knowledge is a kind of practical technology; and if we stand still on a sort of so called the on-paper strategist, and there off to teach the basic theory, that will cause a big lost at the practical skill. In classroom, the students or the audience will feel dull, and so it could not facilitate the usage of the tech. In most of colleges or universities, especially in the school of culture and philosophy, if your course is simply focusing on abstract theory, the effects will be very limited. How to solve the trouble, that is the paper will discuss in forward.

For the purpose, it must to accept some measure and use some intermediate link to solve the problem. Against the computer network usage, a practical technique, first of all, we must emphasize their practice, stress the link of both the theory and application and stress the laboratory experiment. Only if the students learned the practical use in the lessons, and put the theory into practice, they will interest in the course, and consolidate the knowledge in mind, and so in depth understand them.

For achieving to the aim, we have taken some change in the computer network teaching. First, we cut off a piece of the whole course, to set up a particular laboratory experiment lessons called the "Internet Laboratory Works". The destination of the measure are aimed at two aspects: one of them is to enlarge the classroom teaching hours, that will cause the students grasped more details of internet skill; while the other is to enable them to get more internet handling abilities. We hope the students, after the class, will achieve the level of an internet manager. And so it will let them can suit more job in the future. In teaching of the course, we have some bold change and reform as mentioned above and gained the advantage of new measures. The new rule of teaching guidance is not to take much care of daily tests and the scores, so the students gained more joys in process of classroom learning.

II. MEASURES TAKEN FOR SOLVING THE PROBLEM

In the following, we will introduce the key points and the hardness of the course. In practice, the internet lessons contains many contents pertained to the experimentally ones, such as, router theory, data exchange device organization, wireless router configuration, construct internet connector and its test, remelting and connect of optical conductor s as well as their tests, all kinds of servers' configuration, etc. But still there is knowledge cannot be explained by laboratory experiment. For example, there are a lot of conducting protocols (agreements) between users, internet regime construction, how to effectively inform a pair of computers, etc. cannot involved in the teaching. For a better understanding of IP construction and their encapsulation, we try to use network

sniffers, e. g. Ethereal, sniffers etc. as usual. The main purpose of using them aimed at dissecting the scratched IP pack, to look into their internal construction. And then to compare them with the theoretical one, that is to have a completeness of the procedure from theory to practice.

In the following let us take a brief introduction for sniffers:

A. The use of sniffers

Sniffers almost have a long history as internet. It is usually used to collect data set. The data can be a users' account number and his password, also may be a pack of secret data set or the like. As the internet technique gradually spread up to the crowd, and the information safety attracts more and more peoples' concern. And also sniffers play an important role of hidden intruder.

Sniffers is an equipment used to fetch internet data set, so its legal use concludes at analysis of internet data flow, and so to find out existed trouble in the network. For example, if a section of the network runs unusually, some data set transferred a little slow down, and it is unclear where the bad knot resided. At this moment, you can use the sniffers to find the bug out, and so as to eliminate them.

Another important use of sniffers concludes at as an IP pack scratcher, it can be used to look into every practical internet phenomenon, to analyze every internet protocol, as well as data set's encapsulation and its format, if it is reasonable. Still it can be used to understand the stack-layers' construction of the network and their protocol, to analyze the base layers' working principal and its procedure of every network server, to set up reasonable configuration of the servers as well their function' tests, and so forth.

The aim of this paper resided at learning how to use the sniffers to analyze internet protocol.

B. Working principal of sniffers

In general, all of the network interfaces of the same section are able to visit every physical media, and transfer data set to/from it. Every interface has their own particular hardware address, and it is different from others among the web. In the same time, every network system must have a special broadcast address to represent all interfaces address. In normal, a legal interface should be able to respond these two sorts of data frame:

Target area of the frame has their hardware address matching with the local network address.

Target area of the frame must own broadcast address.

When accept either of the above listed data set, network, through CPU interface, will cause an interrupt, and then let the operating system take attention, and it will transfer the data including in the frame to the system to be processed.

Sniffer is a kind of facilitate which can let the local network interface to be become a "promiscuous" state, and then the interface will have the "broadcast address", therefore it will offer an interrupt for every received frame, and let the operating system process every data set, which flow through the given physical media.

So we can see, the sniffer works at the base layer of the network, it can seize every through flowing data set, let the installed software process them, and then analyze the state of whole network doing, and show up the layout of the system.

C. Sniffer's classification

Sniffers can be made up as software and hardware. Hardware sniffer, like FLUKE made, pertained to many kinds of network test apparatus, even though its function are strong enough and perfect, but of course, they are expensive. Software also can be classified into many varieties, most of them are charge free, so they are very broadly applied. Daily used sniffer softwares are: Ethereal, Sniffer, NetXray, Snort, etc. Most of these softwares only suited for some given operating system, like Windows version and Linux version separately.

III. ANALYSIS OF NETWORK PROTOCOL

A. Definition of internet protocol

Internet protocol (IP) is the kernel one of the TCP/IP protocol. All of the TCP, UDP, ICMP, and IGMP data are transferred by the format of IP. IP can offer unreliable, connectionless data report.

"Unreliable" means that it cannot ensure the data flow will be wholly transferred to the destination. IP only can offer good transfer service. If somewhere it happens errors, for example, a router timely used up all of the buffer areas, IP will take a simple measure to blast off the data set. And then it informed the source end. Any needed reliableness must be offered by the upper layer (e.g. TCP).

The term "connectionless" means that IP do not in charge of the state information of the successive data set. Every data report is treated independently. And this explained that IP data report maybe received not accordingly by its lined-up order. IF a data source send out two successive data reports (first A, then B), every data report is independently selected by the router. As the route selected is not the same, so data set B may arrive before set A.

The template is designed so that author affiliations are not repeated each time for multiple authors of the same affiliation. Please keep your affiliations as succinct as possible (for example, do not differentiate among departments of the same organization). This template was designed for two affiliations.

Encapsulation and format of the IP data report

IP data report shows in Fig.1. The head part of a usual IP consists of 20 bytes, except in case of existing optional segment.

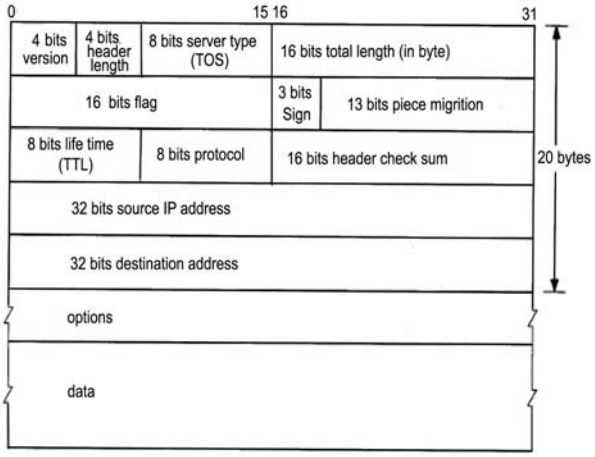

Figure.1. Data report format of the IP

1) Version number: indicates the data report based IP number. Version 4 (IPV4) is the current popular used.

2) Head part length: This domain indicates the length of the heading, which generally occupied 32 bits, including all options. Because it consists of 4 bits in a section, so the longest one of the head part can not be exceeded 60 bytes. Generally, section length of every data report (no options) is 5. Receiver end by this part is informed where the data packet begin and where it is ended.

3) Serving type: In most case users do not use this information. This domain using figures express the importance of the packet. Bigger figure means its priority larger than others.

4) Total length: This domain indicates the factual length in byte of the report. The longest length of a given report would not exceed 65,535 bytes, otherwise it will be ruined by receiver end. By the head part section length and the total length section, the receiver will be informed the start location and the content length of the data packet.

5) Flag: Every data report begins with a signal figure. Ahead of the next report, its value will be increased by 1 accordingly. If the number of the data report is more than 1 (it is inevitable), this domain indicates the serial number of the given data report, sectional data report will held the original ID number it occupied in before.

6) Sign: It consists of 3 bits. From the left, the first one left behind unused, the second indicates DF (Don't fragment), while the third indicates MF (More fragment).

DF= 1,fragment not allowed.

DF= 0, may conduct fragment.

MF= 1, there is fragment data report followed.

MF= 0, no more fragment followed.

7) Piece migration: This domain indicates the migration value in the original data report, its unit counted by 8 bytes.

8) Life time: This domain indicates the allowed transfer time span. In case of errors happened, e.g. if a given data report have been lost in process of transfer, this will inform the sender to do again.

9) Protocol: Thisdomain indicates the upper layer protocol number, which related with the given data report.

10) Check sum of the verification code: This domain indicates the verification is done well by the heading part of the data packet.

11) Source address: indicates the address of the sender machine.

12) Destination IP address: indicates the address of the receiver machine.

13) Option: IP data report as well as ARP data report are the same encapsulated in link access layer data frame. When the "type" section of an Ethernet data frame is 0800, it indicates that the data are of IP type.

B. Using sniffer to scratch IP pack and then analyze it

It is easy to scratch an IP data pack on user's machine. When we did this, and open the data packet, may see the following figure (Fig.2). By the yellow data indications we can see the data pack construction. And at the lower part of the table we can see a 20-byte grey figure expressing the content of the packet. From label 45 through label 89 location, there are 20 bytes in total. According Fig. 2, we can see the IP contents are stored by line. Every line consists of two words, 4 bytes, 32 bits. If you using the grey numbers to fill in the respective position in Fig. 2 in system of binary, then you may understand the real meaning of the figures itself.

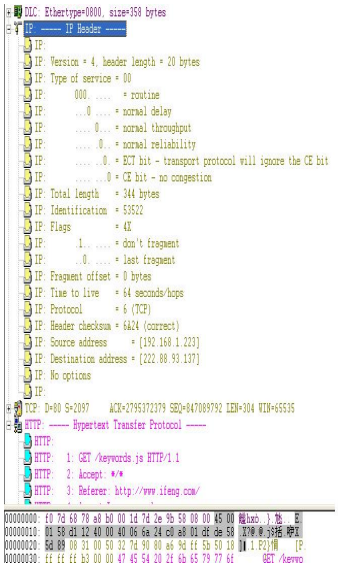

Figure.2. IP data packet

By Fig. 2, we can see that the first byte is 45, the letter 4 means IPV4, while the letter 5 means that the length of the IP equals to 5X4=20 bytes. The second byte 00

indicates the type of the IP and its priority. The third and the forth byte are 01 58, means the packet length is 344 bytes. The fifth and the sixth byte are D1 12, when expressing them in decimal is 53522. This domain indicates the position of the data report. Sectional data pack holds the primary ID number. It says the ID number is 53522. The seventh and eighth bytes are 40 00. Among them, in binary, the first three digits of the seventh bytes indicate the sign digit. The Fig 4 equals to 100 in binary. While the digit 1 mean the data is not allowed to cut to pieces. The successive "0" means that this is the last data packet. The last 0 means nothing. After that the followed 13 each 0 indicates no piece migration exists. The ninth byte is "40", it means that the life time of the data packet is 64 seconds. The tenth byte is "6", it means the upper layer protocol is a kind of TCP. The eleventh and the twelfth byte 6A 24, is the check sum number, that indicates the data packet is correct. The next four ones, 13 through16 bytes are C0 A8 01 DF, indicate the source IP address are 192, 168,1, 222 respectively. The last four ones 17 through 20 bytes are DE 58 5D 89, indicates the destination IP address are 222, 88, 93,137 respectively. [4]

According to the above detail explanation of the internet protocol (IP) example, students will get a thorough understand of the term IP and its uses implied. We use the software sniffers to scratch IP packet, through this way of classroom teaching, it is a vivid lesson. The way by experiment to show up the theoretical meaning, will make easy to understand, and as well promote the enthusiasm of student learning. After four years teaching practice, the aim of reformation has been verified successively.

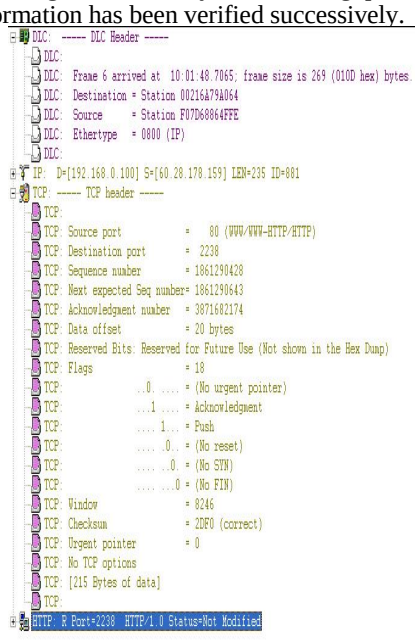

Figure.3.TCP data packet

C. Understand of network construction through IP pack scratching

Through using the sniffer to scratch IP packet, you may have a deepened understand of the network construction. In Fig. 4 presented the stack layers of the scratched data packets.

In Fig. 3 we can see the uppermost layer is the DLC layer, which is the physical one of the network. There are two items, primary computer's and the destination computer's physical address. Besides, it is indicated the length and the arriving time of the records. In the mean time, it fixed the respective information of the former data set's related packet record. In the data packet it fixed the IP address of sender and receiver computer, and also the protocol's number, data packet length, life time of the former layer, etc.

At the upper layer next to the IP packet, it is the TCP, then the HTTP ,its source end number is 80, and the destination end number is 2238, etc. In the upper layer of HTTP, fixed the information related to the HTTP, such as HTTP version number, data packet length, data type etc. Accordance the above listed information, we have depicted the following charts i. e.Fig.4 and Fig. 5 [5].

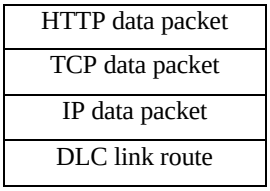

Figure.4.construction chart of pack scratching

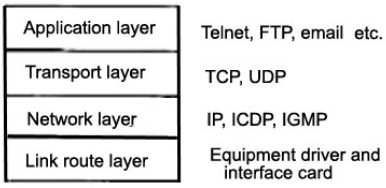

Figure.5.TCP/IP network construction

IV. CONCLUSION

In the network teaching, we may use the sniffer tool to have a better understand of their data packet's construction, such as for TCP, UDP, ICMP, ARP, HTTP, Email, FTPand Telnet. When we open the scratched data packet, all protocol items as listed in detail. Through analysis of the protocol's contents, you can learn how to construct them. In the process of IP packet scratching, you can learn how the network transferring is realized, i.e. to know TCP/IP transferring related knowledge. Besides, in process of packet scratching, we may find some problems among the data pack, such as safety trouble. If a user's name and his password is transferred in a way of plain code, that may be stolen or lost in vain.

REFERENCES

[1] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[2] Xiaoming Zhu,Computer network: technology and applications, China railway press, 2011.

[3] Huan Li, Computer network, China railway press, 2010.

[4] Su Zhou, Technology of network management, China railway press, 2009.

[5] Yang Gao, Computer network: Theory and practice, Qinghua university press, 2009.

[6] Weidong Mo, Computer network: Technology and application, Machine industry press, 2009.