International Journal of Future Generation Communication and Networking
Vol. 9, No. 7 (2016), pp. 1-12
http://dx.doi.org/10.14257/ijfgcn.2016.9.7.01

The Research of P2P Traffic Control Model Based on IPV6

Zhenfeng Qu*

Department of Electrical Engineering and Automation, Luoyang of Science and Technology, Luoyang, Hennan, 471023, China
E-mail:lylonger@163.com

Abstract

On the basis of traffic control strategy put forward by the paper, we designed a model of P2P traffic control based on IPv6, and redesigned the IPv6 header supporting P2P identification, and realized the model of the flow control module which has been proved that this function module can effectively manage P2P business flow with bandwidth management and flow rate limit. The P2P traffic identification and control model in this paper can effectively identify and control P2P business flow in the Internet. So it can contribute to reasonable network planning and effective traffic management.

Keywords*: p2p; control model; IPV6; traffic management*

1. Introduction

Currently peer-to-peer (P2P) [1-2] is widely used has brought a lot of trouble for the broadband operators, because the demand for bandwidth of this kind application is endless in theory, they can make the original run smooth network become more and more congested, not only the network throughput fell sharply, but also greatly change the net flow model, and operation costs are increased obviously at the same time [3]. In that case, the operators used blocking P2P application, or restricting certain application traffic strategy. These measures to a certain extent ease operators' pressure of the outlet flow, but they can't fundamentally solve the contradiction between the users and operators, because they reduce the user online experience for the premise. Traffic is computer network traffic; it is the computer network message flow or packet stream as well. Network congestion means the demand for a resource in the network than the available part of the resources provided in a certain period of time, in a certain layer protocol implementation process. If there are many resources in the network congest at the same time, the performance of the network is obviously degraded; the network throughput will decline along with the increase of input load at this point [4-5]. Network congestion is a very complicated problem; the best way to solve the network congestion is to control flow [6]. Flow control is a general term which put forwarded by some literature, it should include traffic control, congestion control, routing control, timing delay control and so on [7]. Some literature define flow control that it can adjust the sender data transmission rate according to the receiving end can withstand the data transmission rate, to prevent the receiving end data transmission rate more than processing speed at the receiving end, and make network is not overloaded[8-9]. The overall goal of the flow control is effectively dynamic allocation of network resources in packet-switched networks, these resources include processor and buffer in the channel and node switches *etc*. The main flow control functions are as following: To prevent the throughput drop and timing delay by network overload; avoid deadlocking; fairly allocate resources between competing each user *etc*.

ISSN: 2233-7857 IJFGCN

2. Flow Control Technology

2.1. Affiliations

Network traffic control technology is roughly divided into two kinds: series connection control and bypass control. Series connection connects to the network control system, currently application layer flow control is mainly based on the rate plan and token implementation. The scheme adopts step by step based on token window flow control method, do flow control respectively for each different connection. Different connection must book the link between the nodes before the network nodes transmit packets, booking is carried out in the form of the token transfer [10]. A connection can transfer data packets to the next node when it gets the next node token. When a connection does not get a token, it would have to wait. Due to the rapid feedback mechanism between the nodes, instantaneous node cache congestion can be effective in relieving. At the same time, because there is no connection to send packets before getting the token, it wouldn't exist packet loss between nodes. Control scheme based on rate dynamically adjust packet sending rate by end-to-end, although cannot guarantee zero loss rate; it is more simple than scheme based on token, because the token based scheme need complex buffer management algorithm.

The control system of bypass access the network of the application layer flow control technology is not yet mature, it realizes the network traffic control basically according to the characteristics of the TCP protocol, constructing and sending special TCP packet (such as FIN group, RST packet) interrupt application protocols such as part of the TCP connection. Before a connection is established, the user needs to inform network their own business flow characteristics, the network parameters and its demand for service quality, these parameters include: time delay, average speed, and allowed burst length. Once the connection request is accepted, its service quality will get the network guarantees. Because of the lack of network resources could lead to the new requirements of the connection was refused, so the bypass control is sometimes referred to as preventive congestion control, it is suitable for the real-time and multimedia services. But for business data and adaptive multimedia business, bypass control is not suitable [11].Because in the bypass control, even if the network exist residual bandwidth; it can't send packets more than the regulations of the service contract.

$$D = \left| pair.srcport.num - pair.dstport.num \right| \quad (1)$$

For a series connection control system, the implementation of traffic control is easy, but its threat to the network also is bigger, it is easy to cause the network bottleneck, and become a single point of failure. If take discarded message flow control, many real-time streaming media communication will not be able to tolerate, technology remains to be further research in this field. Way to bypass control system is not easy to realize accurate control of network traffic, but it has no effect on the stability of the network itself, paralysis of the monitoring system will not affect the normal operations of the network. This way of bypass access network control of the UDP generally adopt bypass interference mechanism to realize, it is not mature currently.

$$DUP_i = E_s / E_{max} \quad (2)$$

2.2. P2P Traffic Control Technology

Currently the most of Internet transmission flow are TCP and UDP traffic. Usually the so-called critical applications generally use TCP as the transport protocol. Thus ensure the transmission performance of TCP is the key to ensure the

quality of the key business service [12]. TCP is try their best to service delivery for Internet transport layer protocol design, it uses packet loss to trigger, window control, addition increasing multiplication decreasing AIMD (Additional happens Multiplied Decrease) congestion control mechanism to control the flow, this flow control on the one hand lead to the sudden network traffic, on the other hand lead to the rate at which the TCP session itself is very unstable, also make the packet loss is inevitable in the TCP transport. Therefore, we must improve the TCP transmission performance to ensure the stability of the key business flow transmission [11]. UDP is widely used in the Internet for transmission of streaming protocol. The core problem of UDP protocol is that it does not have the transport layer flow control mechanism to regulate (often depend on the application layer), and the lack of UDP traffic flow control can lead to the unfair use of network resources, and affect the performance of TCP traffic. So we must manage the TCP and UDP traffic control, to realize the effective bandwidth utilization.

$$EL_i = \alpha * EL_{i-1} + (1-\alpha)t_i \quad (3)$$

$$EL_j = (1-\alpha)EL_{j-1} + \alpha t_j \quad (4)$$

Straight through flow control is usually in a transparent mode and used by concatenating to equipment in the network. Through the application of the various types of network flow classification and it will discard the P2P traffic packet that needs to be controlled according to the control strategy. Two clients of P2P data transmission did not receive a packet or confirm the information in a certain period of time; it will start using the congestion control mechanism of TCP/IP protocol or application layer protocol for slowing down transmission, so as to realize the purpose of the P2P traffic control. Straight through flow control works as shown in figure1.

Figure 1. Flow Control Way of Working

2.3. Design of P2P Traffic Control

A comprehensive network business flow control strategy is proposed in this paper. Based on this plan, to achieve P2P traffic control, generally has the following several stages: in the first place, test and analysis of network traffic, according to the business matching values to identify the P2P traffic from the network traffic, and control strategies correspond with various P2P protocol, to control and manage the excess of P2P traffic in different ways, to ensure that legitimate users with its identity permissions enjoy the network service quality, to prevent illegal users from abusing network resources. Under the premise of comprehensive analysis on the latest P2P traffic identification, traffic control technology and control strategy, we design a model of P2P traffic control model based on IPv6 in this paper, as shown in figure 2.

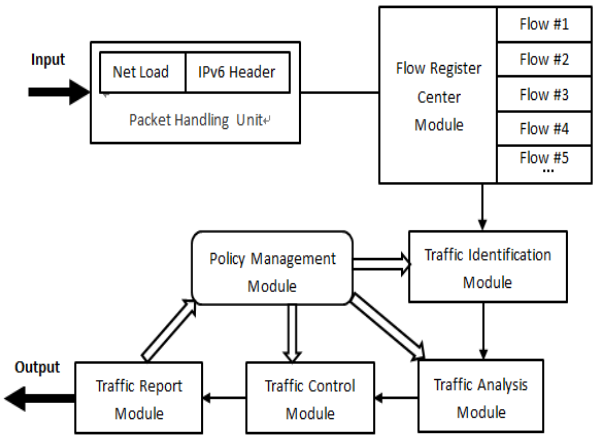

Figure 2. P2P Traffic Control Model

As figure2 shows, the flow control model includes seven function modules: (1)The packet handling unit (PHU) module. This module is mainly responsible for receiving and analysis the coming IPv6 packet, get IPv6 flow label, hop to hop option of s-port and d-port field and other QoS related information and transmit them to the flow register center(FRC). (2)The flow register center (FRC) module. This module is mainly responsible for the new IPv6 packets classification and packets pattern recognition by making use of business recognition engine, fit out of the packets belong to business types of application layer, and complete the flow information (including P2P identification information) of the registration and management. (3)The strategy management (PM) module. This module mainly provides business flow identification strategy and the control strategy of the knowledge base and methods base development, change and implementation, to achieve a certain accuracy through the execution of the business identification and business control. Especially when the network congestion occurs, using different control mechanism for different flow, for example, to take a more strict control mechanism for malicious P2P flow, ensures normality operation of the network. In addition, the flow control also includes the protection of certain business flow and priority. PM based on the intelligent strategy selection mechanism of the feedback, when actual network characteristics change, flow control strategy base can be dynamically adjusted, to implement strategy of customizability and scalability, to drive the flexible and effective traffic identification and control. (4) The traffic identification (TI) module

This module is mainly responsible for the traffic identification; it adopts the traffic identification module proposed in this paper, recognition based on the transport layer connection pattern and detection technology based on DPI for identifying solutions. In addition, still can use two-way identification technology. (5) Traffic analysis (TA) module. This module mainly according to the flow bit rate, flow rate and the number of connections on the analysis of the flow sources and characteristics, and assess the use of network bandwidth resource, efficiency and potential threat, select appropriate control strategies for different types of traffic flow. (6)Traffic control (TC) module. This module is mainly responsible for the quality of service, to limit the bandwidth resources of non-core business (such as P2P), in order to prevent the network resources competition. Common control methods include: based on the service level, based on the flow discarded control, based on flow connection access control, time setting, static/dynamic bandwidth assurance, *etc*. (7)Traffic reports (TR) module. This module is mainly responsible for providing the details of the network operation. It reports the business data

according to various needs, analyzes business data, generates statistical analysis report on regular, saves the data analysis results to the database, and provides the perfect system alarm information, and timely feeds back to the strategy management module, so as to dynamic adjustment and the expansion of traffic management strategies. Traffic identification module and flow control module are the two core function modules of the whole P2P traffic control model, they are also the important research contents of this paper. We has designed a P2P traffic identification model and verified its validity in this paper, this traffic identification model is the implementation scheme as traffic identification module, it will no longer be stated in detail. Here mainly to elaborate the IPv6 header design and the realization of the flow control.

3. IPV6 Header Design

The design of P2P traffic control model is face to IPv6 in this paper, the main problem of network traffic control under IPv6 is that the IPv6 protocol for IP datagram format and IP address representation pattern is different from these of the IPv4 protocol. So in order to realize this technology, it is necessary to adopt the appropriate method, makes the flow of data can be correctly identified and obtained. Due to the header using data analysis method can be implemented for P2P traffic identification and control, we design IPv6 header relative fields in this paper, so as to realize the identification of P2P traffic under IPv6, leave P2P traffic identification and control can be done in the same layer (IP layer), which helps to improve the effect of P2P traffic management, reduce the complexity and processing spending.

IPv6 defines the concept of data streams, a data stream from a specific source side to a specific unicast, broadcast or multicast destination end of series of grouping. The source end requests to do a special processing about grouping packet in the middle of passing all nodes. These special processing can be done by a control protocol, such as resource reserve, distinguish services, traffic engineering mechanism or through group carrying on message across to the router.

IPv6 header contains a length of 20 bits flow label field, be used to identify the data packets that belong to the same business flow. Although a terminal node can at the same time as a source of multiple business flow, flow label, source and destination addresses can uniquely identify a business flow. Flow label field can be used to identify the data flow, to support quality of service. IPv6 allows end users to use the field of communication quality request, the router can identify all the data packets that belong to a particular data flow according to the field, and provide specific treatment for these groups on demand, the effective processing data packet flow mechanism is especially useful for real-time applications. As the data flow identity information is included in the IPv6 header, even data packet with IPSec encryption can obtain QoS support. After basic IPv6 Header is hop to hop option extended Header, it is identified by zero the value of next header field in the basic Header, each router contains a packet forwarding path to detect optional information.. Hop to hop option can be used to carry important information related to the QoS. The flow label value set is divided into three categories in this paper: (1) Zero value, flow label value setting to "0" is not of the nature of flow data message, according to the traditional way of the best processing, no guarantee QoS, low priority, could be discarded by middle forward equipment at any time; (2) A specific value], designed for specific applications such as VOD, video conference, P2P *etc* to retain flow label value set. The specific value of the data packet will be in accordance with the quality of service requirements and processing in the contract; (3)Other values, it is necessary to choose a pseudo random value from 1 to FFFF hexadecimal number. Forwarding processing according to one or more related to the flow properties, these properties may include flow type, the label value, source address, destination address, the TCP/UDP port

number, one or more extended header, *etc*. May also include the external environment constraints about flow, such as the network administrator to choose the parameters of the flow of packet forwarding. For this purpose, you can use the beginning of IPv6 flow label 3 bit defines the methods of use, the remaining 17 bit is used to define the specific methods used in the format. Therefore, when a user uses P2P software, data packets are sent and received by explicit identification of P2P applications. As the only global IPv6 address can receive and analysis into the IPv6 packet, get IPv6 flow label, jump to jump option are enough to show that user's identity, so explicit identification of P2P applications is not only for the convenience of P2P traffic control, but also for protecting specific users with a higher quality of service requirements.

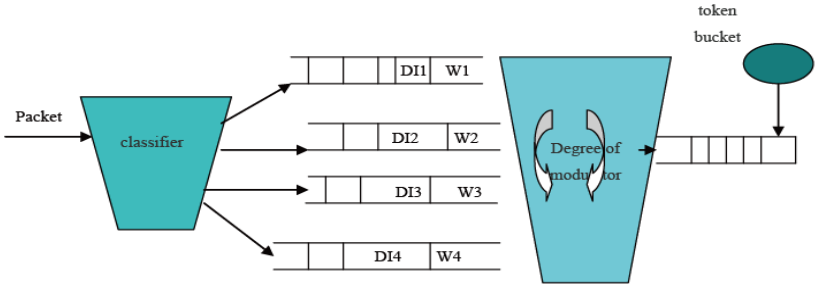

Figure 3. The Realization of the Flow Control Module Framework

Flow control module has its unique position on the function, at the same time; its performance and stability are also related to the performance and stability of the whole system. As shown in figure 3.3, the realization of flow control module frame. The classifier is the set of classification rules and classification strategy, its implementation is not required. The following is the main detailed description of submodules implementation of queue scheduling and traffic shaping of flow control module.

Scheduling [6] is one of the core mechanism of system resource management, it is the effective means to solve the problem of resource sharing in multiple business competition. Queue scheduling manages the link bandwidth, and determines to choose which packet forwarding in a waiting queue according to certain rules, makes all input business flow share output of link bandwidth according to scheduled way. Queue scheduling affects the main performance parameters including bandwidth allocation, delay, delay jitter, *etc*, it is one of the core technology of the network quality of service control.

Through the analysis of the existing mature queue scheduling algorithm, we compare their respective advantages and limitations, and finally choose DWRR algorithm as the implementation algorithm of queue scheduling module in this paper. DWRR algorithm is a relatively simple,the cost of realization of this algorithm is not high, the computational complexity is not high, and also do not need to maintain a large amount of status information, it can be used in the hardware implementation, and it is suitable for high-speed network router, and can provide precise bandwidth allocation, to meet the requirements of differentiated service. In addition, to prevent the lower priority service class from not getting service during long time by ensuring each service class to get the user configuration of the output port bandwidth, overcome the deficiency of the priority queue, to ensure the fairness for the low priority queue, so we select the DWRR algorithm as the implementation algorithm in the queue scheduling management module. But the support of the DWRR for end-to-end delay and delay jitter is not enough, in order to improve the DWRR performance in this aspect, this paper puts forward the improved algorithm ADWRR based on DWRR algorithm (Adaptive queue scheduling algorithm),it is trying to solve the problem of end-to-end delay and delay jitter, to reduce the end-to-end delay and delay jitter control in an acceptable range.

ADWRR algorithm is the improvement on the basis of DWRR algorithm, as shown in figure4. Its basic idea is: introduce two parameters for each queue i, respectively are: a

weight value Wi, delayed Index (Delay Index) DIi. DIi is ratio of queue length of i and the assigned weight value of Wi, namely the DIi = QueueLengthi/Wi. Scheduler calculates each queue DI value after every a certain time Δt, descends order of all DI values, the scheduler serves queues according to DI value from high to low. When the number of active queue change, the scheduler must recalculate queues DI value, descends order DI value, serves queues according to DI value from high to low. Because each queue DI value is a dynamic change, so the scheduler service queue is dynamic changes as well.

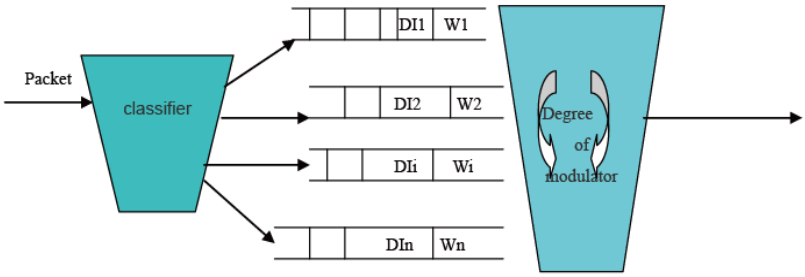

Figure 4. ADWRR Algorithm Diagram

As shown in figure4, the packet inserts into a different queue through the classifier, in ADWRR algorithm, to maintain two parameters Wi and DIi for each queue. Assumptions at time t, scheduler service order is (1, 2, 3,..., n), after time Δt, it recalculate each queue DI value, the scheduler serve each queue from high to low in the same way as DWRR algorithm according to DI value of high and low, In some real-time multimedia application flow, that can reduce the packet delay jitter, and to meet the requirements of the quality of service well.

4. Test and Analysis

The experiment platform in this paper is the Linux + NS2.27. NS, starting from version 2.26,it can only be runner under the Linux environment or the Linux environment simulation. Experiments adopt the simulation topology structure as shown in figure 5.

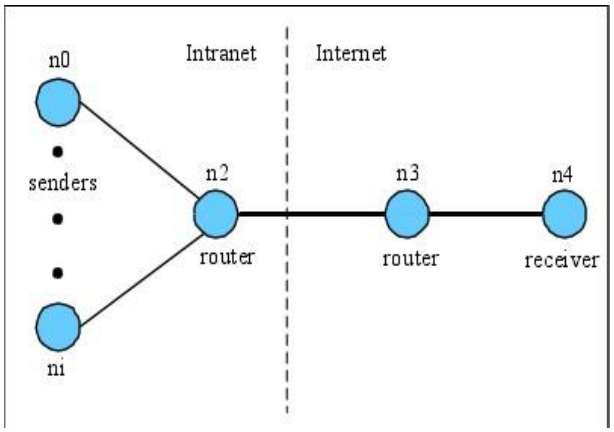

Figure 5. Simulation Network Structures

These simulation networks simulate a connection between campus network and Internet, a dotted line on the left is on behalf of the campus network, the right is on behalf of the Internet. The n2 and n3 are on behalf of edge gateway, the queue scheduling algorithm DWRR and ADWRR are applied to the edge gateway n2. On the left n2 are the data senders (senders), n4 is the data receiver (receiver). Each node of the campus Intranet

n0, n1,…ni are set to 10 MBPS speed, the link rate between n2 and n3 is set to 1 MBPS, this link simulate network bottleneck, the receiver n4 link rate is set to 10 MBP .

The queue scheduling module of flow control module is applied to the edge gateway in Experiment. Respectively adopts the DWRR queue scheduling algorithm and ADWRR queue scheduling algorithm to do comparison experiment in the queue scheduling module. The types of data flow in network simulation mainly include video streaming, FTP stream flow and other background stream flow, on behalf of the other application traffic on the network. The experiment measure the main parameters of the video stream end-to-end transmission delay and delay jitter, because these parameters has the very vital significance for multimedia real-time business service quality. In order to as far as possible to the real network environment, meanwhile considering the limitations of simulation experiment, some parameter settings are as follows: video packet size is 200 KB, video streaming transmission speed is 320 KBPS; FTP stream flow data packet size is 400 KB. Background flow data packet size is 100 KB (according to the survey, the data packets of network transmission are less than 128 KB, and they are about 54%), the rate is 160 KBPS.

This experiment simulates a video conference, multiple nodes at the same time send video stream, and there are also a FTP flow on the network and other types of traffic.

P2P traffic control model are proposed according to the above, a small local area network (LAN) is set up in this paper, the model of the flow control module performance test experiment is carried out, experimental environment as shown in figure 6.

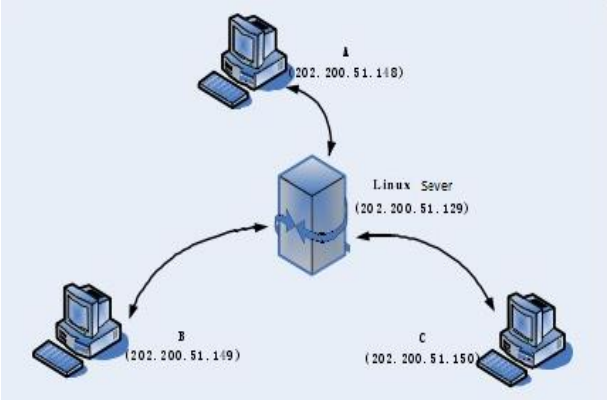

Figure 6. P2P Traffic Control Environment

In A small local area network (LAN), there is a Linux host server, there are three Windows client A, B, C. Using Linux2.4.18 as a server operating system, using C language as the development language of system, the flow control strategy is deployed on Linux host, so as to flow control mechanism of Linux supports P2P traffic control model of this paper. In a NetMeter software is installed on the server at the same time, as the traffic statistical tools, it carries out statistical analysis on the LAN traffic condition.

After the whole local area network (LAN) running stability, three clients in T time to begin their own online business at the same time. The client A begins to do FTP download and e Donkey download; Client B starts Skype chatting and browsing; The client C starts browsing the web and the BT download . At T 'time (two minutes later) , to do statistics of network traffic situation as shown in figure7、figure8 and figure9. At X time, to do queue scheduling management strategy for Linux host server. At X 'time (two minutes),to do statistics of network traffic situation as shown in figure 3.9.At Y time, to undo queue scheduling management for Linux host server, take statistics of network traffic, as shown in figure 9.

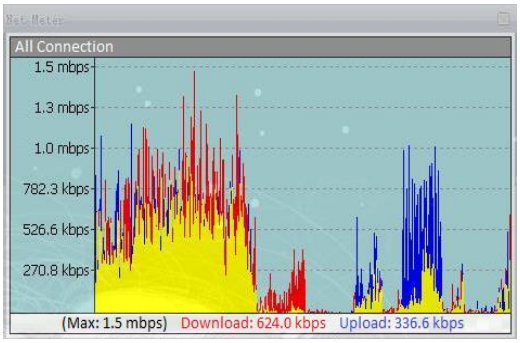

Figure 7. Time=10, Network Traffic Transmission Speed

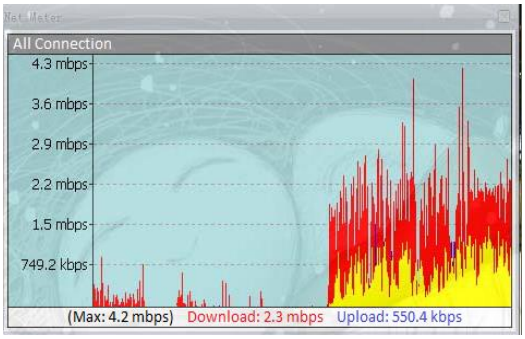

Figure 8. Time=20, Network Traffic Transmission Speed

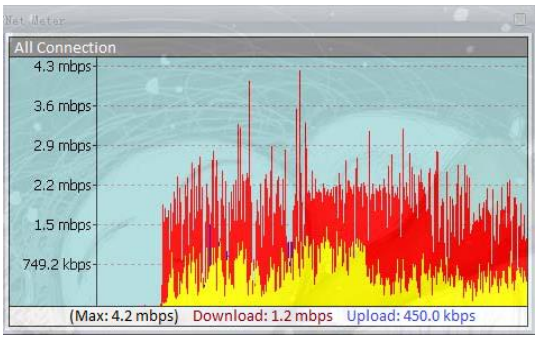

Figure 9. Time=30, Network Traffic Transmission Speed

It can be seen from the comparison analysis of Figure 7, Figure 8 and Figure 9 that all in the bandwidth traffic up to 4.2 MBPS at TT 'time, most of them are P2P traffic. After the implementation of queue scheduling management at X time, ,P2P services of bandwidth is significantly lowed, LAN total bandwidth already falls to 1.5 MBPS at X time, basic bandwidth balances in 1.0 MBPS during XX' period, it has reached the peak bandwidth allocation strategy. At Y time, after the revocation of queue scheduling management, P2P services of bandwidth increases to 4.2 MBPS, takes up most of network bandwidth.

The experimental results show that the model of queue scheduling management module can effectively implement the bandwidth control and management strategy, limit and reduce the P2P business high bandwidth, so as to ensure the normal conduct of other key network service.

5. Conclusion

On the basis of the research of P2P network business flow control technology, a model of P2P traffic identification and control based on IPv6 was proposed and

designed in this paper, this model is composed of seven function modules, including traffic identification module and flow control module are the two cores of modules. In order to realize P2P traffic identification based on IPv6, firstly IPv6 header that supports P2P traffic identification was designed. Secondly, the queue scheduling sub-module and traffic shaping sub-module of flow control module were implemented. Finally, the model performance test experiment was carried out. It was proved by experiments in this paper that the design of flow control module can effectively implement P2P business flow bandwidth management and flow rate limit. So it can contribute to reasonable network planning and effective traffic management.

Acknowledgements

The authors wish to thank Science of Technology Research of Foundation Project of Henan Province Education Department under Grant Nos.2014B520099; Natural Science and Technology Research of Foundation Project of Henan Province Department of Science under Grant Nos. 132300410023; Youth Fund Project of Luoyang Institute of Science and Technology (Project No. 2013QZ02).

References

[1] W. Wu, J. Liu and R. Ma, "On incentivizing upload capacity in P2P-VoD systems: Design, analysis and evaluation", Computer Networks, vol. 57, no. 7, **(2013)**, pp. 1674-1688.
[2] Y. Zhou, T. Fu, D. Chiu, "On replication algorithm in P2P VoD. IEEE/ACM Trancation on Networking", vol. 21, no. 12, **(2013)**, pp. 233-243.
[3] W. Wu and J. Liu, "Exploring the optimal replication strategy in P2P-Vod Systems: characterization and evaluation", IEEE Transactions on Parallel and Distributed System, vol. 23, no. 8, **(2011)**, pp. 1492-1503.
[4] B. Cheng, S. Lex, H. Jin, X. Liao and Z. Zhang, "GridCast: Improving Peer Sharing for P2P VoD", ACM Transactions on Multimedia Computing Communications and Applications, vol. 4, no. 1, **(2008)**, pp. 55-59.
[5] J. Yan and X. Fan, "HFBP: Identifying P2P traffic by host level and flow level behavior profiles", Journal of Networks, vol. 8, no. 8, **(2013)**.
[6] K. Xu, M. Zhang, M. Ye, D. M. Chiu and J. Wu, "Identify P2P traffic by inspecting data transfer behavior", Computer Communications, vol. 33, no. 10, **(2010)**, pp. 1141–1150.
[7] T. Do, K. A. Hua and M. A. Tantaoui, "Robust video on-demand streaming in Peer-to-Peer environments", Computer Communications, vol. 31, no. 3, **(2008)**, pp. 506-519.
[8] Y. Guo, K. Suh, J. Kurose and D. Towsley. "DirectStream: A directory-based peer-to-peer video streaming service", Computer Communications, vol. 31, no. 3, **(2008)**, pp. 520–536.
[9] P. Andrea, "A Survey on content-centric technologies for the current Internet: CDN and P2P solutions", Computer Communications, vol. 35, no. 1, **(2012)**, pp. 1–32.
[10] C. Z. Songying and Z. Naiyan, "Research on the Influences of Insulation Technology by Plastic Greenhouses on Working Temperature in aeration tanks in Cold areas in winter", International Journal of Heat and technology, vol. 33, no. 1, **(2015)**, pp. 181-186.
[11] F. Dai, X. Bao and W. Han, "Reliability Evaluation Method for IP Multicast Communication under QoS Constraints", China Communications, vol. 8, no. 5, **(2011)**, pp. 79-87.
[12] D. Wang and K. Y. Chao, "Superchunk-Based efficient search in P2P-VoD system", Multimedia IEEE Transactions, vol. 13, no. 2, **(2011)**, pp. 376-387.

Author

Zhenfeng Qu, he was born in 1977 in Nanyang City Henan province. In 2009 graduated from Taiyuan University of Science & Technology, Master of Science; He is a lecturer in Luoyang institute of Science and technology of Electrical Engineering and Automation. The main research interest is industry automation, automatic control.

