

<http://ansinet.com/itj>

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSI*net*

Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Design and Implementation of the Campus Network Traffic Monitoring and Analysis

¹Hsin-Te Chan and ²Man-Ting Ku

¹Center for General Education, Tainan National University of the Arts, Tainan, 72045, Taiwan

²Department of Digital Media Design and Management, Far East University, Tainan, 74448, Taiwan

Abstract: In recent years, with the development of optical technology in networking the tremendous demands for bandwidth is increasing on the network deployment from the backbone to campus intranet. In contrast, the campus network deployment has been very popular, all units within the network is also increasingly a large, complex related network applications rapidly increase, it is undoubtedly a serious test for the unit network administrator. This study is a practical study, analyzing that the existing campus network of domestic institutions may encounter problems. The National Tainan College of Art, for example, describes their experience to build the campus network bandwidth management and traffic control mechanisms, the current situation problems encountered and solutions, etc.

Key words: Bandwidth management, network management, flow control

INTRODUCTION

With the increasing popularity of Internet, Internet use has also experienced rapid population increase, according to the Ministry of Economic Affairs commissioned the e-commerce applications for Taiwan Network Information Center, ECRC-the FIND "Taiwan's Internet population questionnaire". The survey shows as of the end of September 2013, Taiwan's Internet population continues to grow, reaching 17.98 million, accounting for 77.09% of all Taiwanese population. This ratio is slightly worse than Japan (79.5%) and South Korea (82.5%), ranked third in Asia, slightly better than in Hong Kong (74.5%) and Singapore (75%), Commercial Internet accounts exceeded 26 million (Yin *et al.*, 2012) as shown in Fig. 1., the rate of increase is quite amazing.

The rise of the Internet to bring with it a great convenience and lifestyle changes, also caused a great impact on the campus, students rely on for the network, making the utilization of the network to continuously improve flow dramatically increase, resulting in reduced network traffic and overall network performance problems occur. However, due to network systems and equipment scattered everywhere on campus, when the network gradually expanded the scale, the bandwidth increasing demand, how to effectively manage the network, the master network conditions to ensure the smooth flow of the network, avoid network resource misuse and timely disposal of the control network is an important issue for the network center managers.

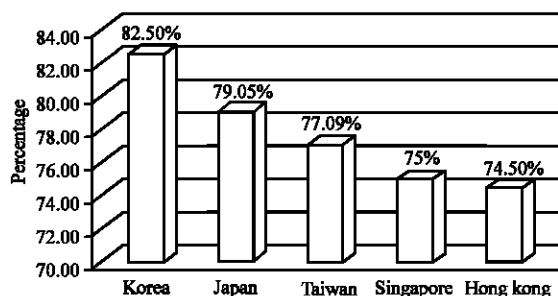


Fig. 1: The ratio of internet users in Asia

Therefore, this study, the author services unit, for example proposed a network architecture, by the IP network management, traffic control and bandwidth control, not only to provide quality of service specific network application framework, but also could solve the problem of IP theft, the Internet network resources is improper use of network bandwidth congestion ... problem.

The main purposes of this study are as follows: (1) Explore the domestic universities and colleges campus network may encounter problems and solutions. (2) To understand the build of the campus network bandwidth management mechanism and may encounter problems and solutions.

THEORETICAL DISCUSSION

SNMP: Simple Network Management Protocol (Simple Network Management, the Protocol, SNMP), first edition

is defined by RFC1157 in May 1990 completed the development of the SNMP Version 3. SNMP network management model is designed for distributed network architecture. Scholar Darryl pointed out that SNMP is used for network management information between two or more network nodes Transfer Protocol, SNMP-managed node is any device on the network allows SNMP access to all of its management information. SNMP itself is a protocol rather than a language which is a set of rules to convey information between entities (Chen, 2012).

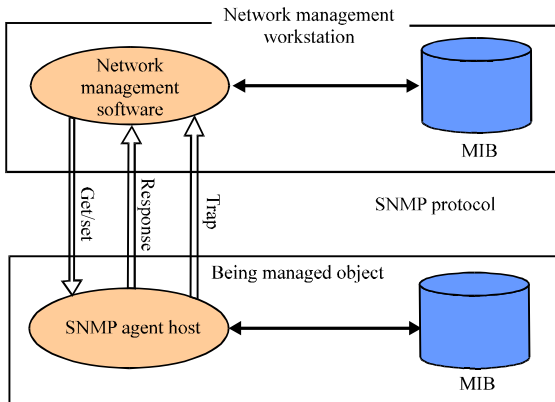


Fig. 2: SNMP main components

An SNMP network management system has three main components, the relationship shown in Fig. 2.

MRTG: The Multi Router Traffic Grapher is a tool to monitor the router traffic, it will the router handle the traffic volume chart shows, allows network managers to know the status and trends of the traffic on the network (Wei, 2013). MRTG to via SNMP the protocol and specify the Router to communicate by Router on MIB to get some statistics related to network conditions. The device which must be SNMP-enabled, will have a Management Information Base (MIB) to look up the OIDs specified. After collecting the information it will send back the raw data encapsulated in an SNMP protocol. These statistics to chart processing, GIF image and HTML page to the browser (Peng and Chen, 2011), as shown in Fig. 3.

RESEARCH INTERVIEWS AND RESULTS

Interview subjects: In this study, telephone interviews with domestic 33 state universities, 15 private universities and 12 technical colleges in charge of the campus network management or contractor personnel, the main content for the school campus network bandwidth management mechanism built set and the problems encountered and so, for the depth interviews.

Results: Interviews results are summarized as Table 1.

Table 1: Interviews results

Description			
Problem	Status	Quantity	Method
1	Has been to build	24	IP + MAC Port + MAC IP + MAC + Port
	Under construction	21	Has been planning to build
	Not implemented	15	Mining DHCP to unregulated
2	Has been to build	27	Management through a Proxy of mechanisms. Mining independent distributed network diversion structure. Develop their own network traffic control system. The procurement of network bandwidth/policy management servo host.
	Under construction	15	Has been planning to build
	Not implemented	18	Only monitoring to inform no flow control
3	Usage limits	36	School regulations vary 1000Mb 1/day 12 1000Mb 1/day 24
	No usage restrictions	24	Only monitoring to inform
	Issues		Solution
4	Network IP theft		Build the campus network management mechanism
	Network resource is inappropriate use, such as: a large number of transmit data		Build a campus network bandwidth / traffic control mechanisms
	Network intrusion/attack		Build Fire Wall or IDS System
5	Computer transmission of the virus		Build a campus network anti-virus system
	The proliferation of spam		For the Mail host control
	Funding support		Strong support for the attitude of the executives
6	Professional IT team		
6	The system implementation is completed, the professionals in the system maintenance vendors with management and co-ordination is indispensable to the success factors		

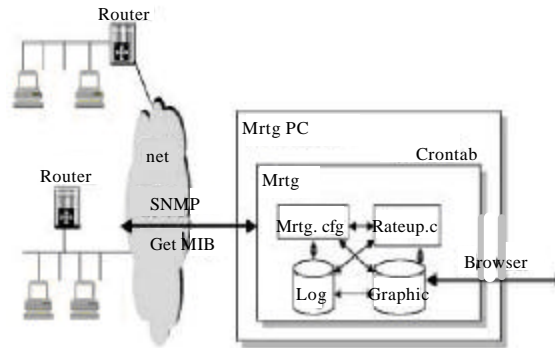


Fig. 3: MRTG operation diagram

SYSTEM ARCHITECTURE AND PROCESSES

Planning of this system contains the IP network management, bandwidth and traffic control, it is described as follows:

Network IP management: Network IP management, to enable students to apply for the IP address and view or modify the application data over IP application process, students are required to fill in the network card MAC address and live floor, contact telephone ... information and check whether their personal data misuse confirm immediately after the completion of the application process. NIC card number all the IP addresses corresponding to the first network management personnel are set as a default value (set to "0"), so no Internet access until the student to complete the IP application procedure without the application user system administrator to check the information is correct, namely the Core Switch OR, Layer 3 Switch), the use of static ARP table records the IP address and NIC card number (MAC address) lock, then apply for The IP can be opened.

Through this mechanism using static ARP record, it can be determined whether the computer of the campus within the Internet. This approach can prevent users to steal other people's IP address the situation, to achieve the purpose of controls.

Network traffic control: The main method Shown in Fig. 4. (1) The use of Layer 3 Module Switch Function to use its built-in flow control for each Port. (2) Function bandwidth management servo hosts.

Network bandwidth control: The main method Shown in Fig. 5. (1) The use of Layer 3 Module Switch Function

to use its built-in flow control for each Port. (2) Function bandwidth management servo hosts.

Transmission of traditional IP networks, "best-effort (Best Effort)", Due to the limited impact of the school's external network bandwidth, has been unable to meet different kinds of application Quality of Service requirements, such as: held a video conference, the school admissions system host, web host and the need to ensure bandwidth network to achieve specific needs.

Therefore, the use of the bandwidth management servo host, to the shortcomings of IP network bandwidth make full use of management and Internet applications, shown in Fig. 5.

SYSTEM ARCHITECTURE AND PROCESSES

Initialization: Firstly, the ARP the Table to fill all the available IP address will fill in the MAC portion of all "0000000 00000 ", as show in Fig. 6.

Flow control setting for the Port or IP, can be divided into two parts: (1) Switch Layer 3 Module to use its built-in Function Flow Control for each Port. (2) Function bandwidth management servo hosts for each IP flow control as shown in Fig. 7.

After completing the flow control action against: The school a one or more segments, the Department and even specific IP or host and different Quality of Service, as show in Fig. 8.

After the completion of the above three steps: According to the information set by the policy servo host to network traffic analysis (Fig. 9) and bandwidth management ... and so on. The host of this policy servo is constructed in the

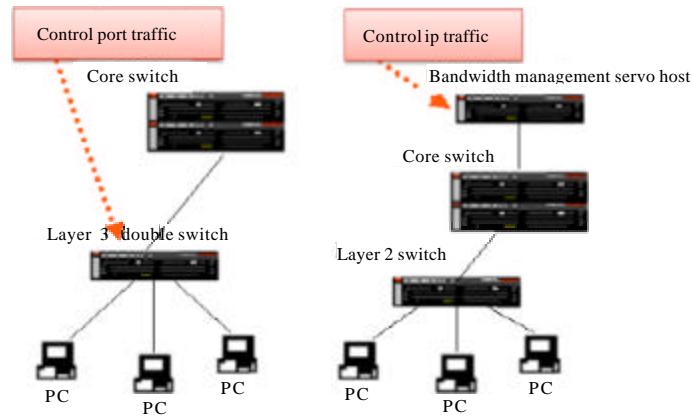


Fig. 4: Network traffic control architecture

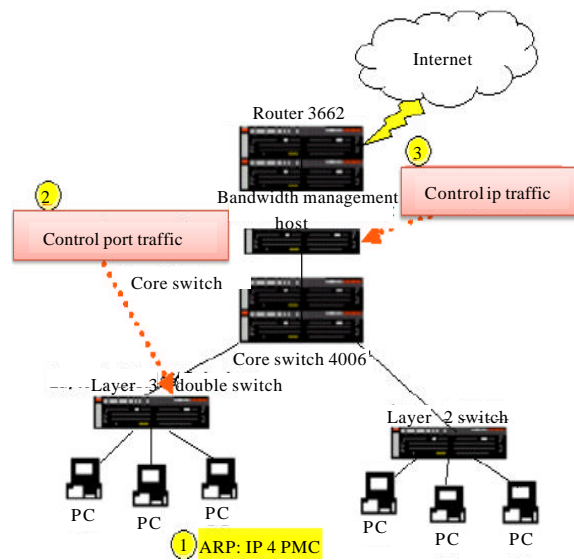


Fig. 5: Bandwidth control architecture

```

arp 192.168.133.21 0000.39e3.65a1 ARPA
arp 192.168.13.101 0060.9767.9297 ARPA
snmp-server community public RO
?
line con 0
transport input none
line aux 0
line vty 0 4
access-class 20 in
password taifon
login
?
end
    
```

Fig. 6: Example of ARP table

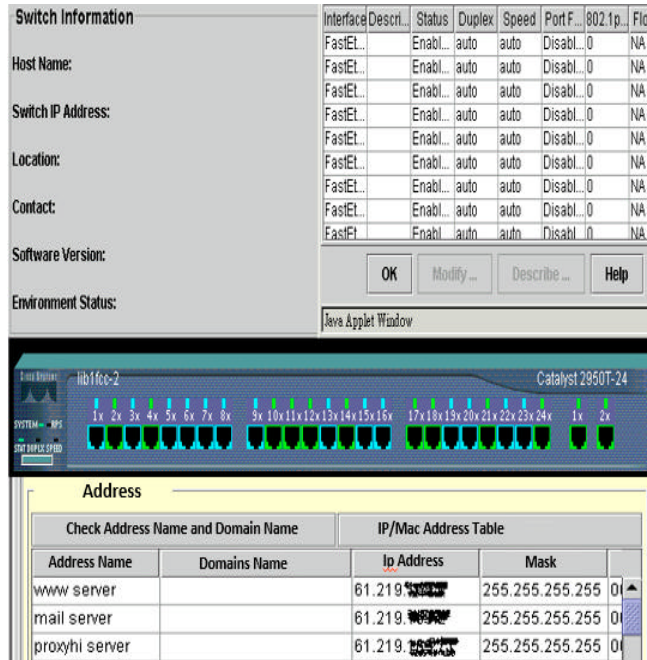


Fig. 7: L3 switch flow control function

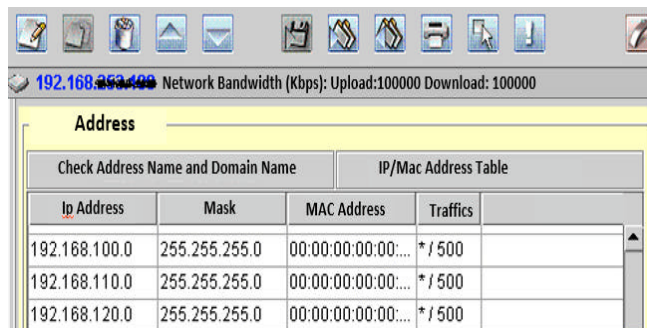


Fig. 8: Specific IP or host QoS

Linux Base server database using MySQL, so it can all flow of information are stored in the Data Base for future statistical analysis.

RESULTS

Ministry of Education is actively promoting the new generation of broadband backbone network, in order to effectively utilize the new generation of broadband, to prevent the improper behavior of the network and require schools at all levels must be completed before the application to join the list of the requirements of network traffic statistics. Therefore, under the framework of this study, in addition to the advantage of setting a static ARP

Table records to prevent students from theft further traffic/bandwidth management mechanisms to provide a feasible solution to apply for a new generation of broadband backbone network needs in this research framework to achieve the following functions:

- Provide the network to use the excess list query
- Lock the card function for the excess and improper user
- The user's IP traffic queries, query real-time traffic
- Traffic monitoring, backup traffic and logs the function
- Produce the total flow (day / week / month), ultra-flow list and rank the list of protocol rank



Fig. 9: Network traffic analysis charts

Table 2: Problems and solution

Problem	The solution
Network equipment used to store configuration data Memory is not large, so once set multiple static ARP record the current settings will not be stored together	Network according to the actual IP needs to cut into sections, in order to reduce the record in the ARP Table
Students malicious conflict with the IP, the system will be clash of IP closed, affect the normal use of the original user	As far as possible By Port IP+MAC records set in the bottom of the Switch Mining the IP+Port+MAC mechanism, will record set in the bottom of the Switch
IP default 000000000000 easily students theft	Randomly select 12 numbers as a default the MAC #

- Record the user's basic information (such as the NIC card number, use the IP, the user's basic information, etc.)

Mainly encountered in the course of the study the following questions and provide a solution for the school as a reference for future build, as shown in Table 2.

CONCLUSIONS

Network management the ultimate aim is to manage dispersed in a variety of resources on the network, the school is small, but the units and taste, so the network build with other schools did not have a considerable extent on differences in expectations of the school experience of domestic institutions, real help, the future will be towards the direction of system automation.

REFERENCES

Chen, Y.R., 2012. An SNMP-based ARP spoofing detection and blocking system for local area network. Master's Thesis, Chang Gung University, China.

Peng, Y.S. and Y.C. Chen, 2011. SNMP-based monitoring of heterogeneous virtual infrastructure in clouds. Proceedings of the 13th Asia-Pacific Network Operations and Management Symposium, September 21-23, 2011, Taipei, Taiwan, pp: 1-6.

Wei, H.Y., 2013. Taiwan's third highest penetration rates in Asia. Business Times, Taipei, Taiwan.

Yin, J., Y. Li, Q. Wang, B. Ji and J. Wang, 2012. SNMP-based network topology discovery algorithm and implementation. Proceedings of the 9th International Conference on Fuzzy Systems and Knowledge Discovery, May 29-31, 2012, Sichuan, China, pp: 2241-2244.