Intranet Performance Monitoring and Problem Solving Analysis with Network Parameters from SNMP and NetFlow

Panisara Treesorn[1] and Suwat Pattaramalai [2]

***Abstract* —** The method for solving the problem of network traffic latency with SNMP and NetFlow parameters is proposed. The analysis is taking experiment in the big communication organization in Thailand. The SNMP parameters can show an accuracy of the connection and the anomaly on router. While NetFlow parameters can show the rate of traffic flow such as: Source IP, Destination IP, Application, Port, Protocol and Traffic. By monitoring router, all mention parameters can inform the network characteristics of the router. The router is monitored with Solarwinds program to pull SNMP parameters and with NetFlow analysis program to pull NetFlow parameters of network. Then these parameters are analyzed by referring to the policy of organization network. As a result, these parameters provide enough information to administrator for managing the network. The problem can be specified correctly and solved to improve the organization network performance.

***Keywords*—**SNMP, NetFlow, Performance, Router, Protocols, Port TCP-UDP.

I. INTRODUCTION

NETWORK system is importance in a large organization to be accessed for internal - external data rapidly and accurately. The network administrator is required to control, diagnose, debug and improve efficiency the network devices. Nowadays, this problem in organization network is a utilize traffic latency to internal system and internet. The traffic monitoring with PRTG in the organization network can show the graph of traffic only which is not sufficient for analysis. Generally, research network monitor focus data flow on the router because it indicates behavior in communication network. Largely, the data capture methods and the analysis is the behavior monitoring on the router with data capture such as: Ethereal, WinDump, Etherpeek, Observer and Sniffer-Pro etc. [1]. The network monitoring is an important activity for the network management. In network data detector, independent developing program simulates patterns of traffic, amount of data and CPU, to consider data flow of Source-Destination IP, Protocol and Port number [2]. There is a study of the basic of NetFlow for traffic monitoring and analysis with NfDump by simulation on the computer with two CPUs, 1GB/s memory speed, 20Gbps link to the main network, and data less than 400 MB per 5 minutes [3]. In [4], detail of network monitor, data processing, analysis and improve efficiency of data collection is presented. In [5], the network performance is monitored from data Flow on the router and the traffic behavior analysis with NetFlow Analysis program installed on Linux operating system. The method to bring parameter values obtained by NetFlow from the router and the results of ping test packet with TCP-IP ACK is analyzed in conjunction with calculation the network performance of devices shown in [6]**.**

Therefore, this research is applied the basic idea and principles of the research papers mentioned above and presents network performance monitoring and problem solving with network parameters using Solarwinds to pull SNMP parameters that indicates of status and security on the router and NetFlow Analysis to pull NetFlow parameters of traffic on the router. This proposed method is a fast information retrieving, convenience for implement, easily for solving the problem of the network and able to modify configuration devices in the network referring to the organization policy.

II. THE PRINCIPLE OF SOLVING PROBLEMS

A. SNMP-MIB

The SNMP architecture is comprised of two basic elements, management stations and network elements. The manager is a console by which the administrator performs his management responsibilities, monitoring and controlling the network elements or agents. Specifically, “SNMP is the communications protocol that allows the console and agents to communicate.” Since SNMP is designed, as its name implies, to be simple. The User Datagram Protocol (UDP) is chosen as the transport protocol for the SNMP message frame. SNMP uses the well-known UDP ports 161 and 162.

Management Information Base (MIB) is a standard for managing the system which each operating system will be implemented. This MIB contains information about the system

Panisara. Treesorn, is with the Faculty of Engineering, King Mongkut’s University of Technology Thonburi, 126 Pracha Uthit Rd., Bang Mod, Thung Khru, Bangkok 10140, Thailand (author phone: +668 9305 3622; e-mail: ps.nisara@gmail.com).

Suwat. Pattaramalai, is with the Faculty of Engineering, King Mongkut’s University of Technology Thonburi,126 Pracha Uthit Rd., Bang Mod, Thung Khru, Bangkok 10140, Thailand (corresponding author phone: +66 2470 9079; e-mail: suwat.pat@kmutt.ac.th).

such as the number of interfaces and so on. There is also a standard MIB for printer. The SNMP agents for different types of devices provide access to objects that are specific to the type of device. In order to enable the SNMP manager or management application to operate intelligently on the data available on the device, the manager needs to know the names and types of objects on the managed device. The Structure of Management Information (SMI) is described in RFC 1155 "Structure and Identification of Management Information for TCP/IP-based internets" shown in Fig. 1.

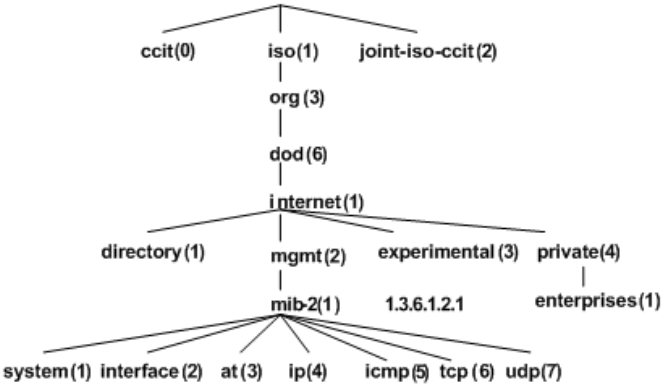

Fig. 1 Structure of Management Information (SMI)

RFC 1213; "Management Information Base for Network Management of TCP/IP-based internets: MIB-II) for use with network management protocols in TCP/IP-based internets." All SNMP agent and tool distributions should include MIBs that will comply with MIB-II and all devices should at the very least return values that comply with the MIB-II standard (see Table I).

TABLE I
Managed Object Groups in MIB-II

Group	OID	Comment
system	{mib-2 1}	General information about device for administrative purposes.
interfaces	{mib-2 2}	Keeps track of each interface on device.
at	{mib-2 3}	Address translation (only for backward compatibility).
ip	{mib-2 4}	Tracks IP (internet Protocol) aspects
icmp	{mib-2 5}	Tracks ICMP (Internet Control Message Protocol) aspects.
tcp	{mib-2 6}	Tracks TCP (Transmission Control Protocol) aspects.
ucp	{mib-2 7}	Tracks UDP (User Datagram Protocol) aspects.

B. NetFlow

IP Packet attributes used by NetFlow in each packet which is forwarded within a router or switch is examined for a set of IP packet attributes. These attributes are the IP packet identity or fingerprint of the packet and for determining if the packet is unique or similar to other packets. Traditionally, an IP Flow is based on a set of 5 and up to 7 parameters. The IP packet attributes are IP source address, IP destination address, source port, destination port, layer-3 protocol type, class of service and router or switch interface. Network information is condensed into a database of NetFlow information called the NetFlow cache. Traffic flow in the NetFlow cache is shown in Fig. 2.

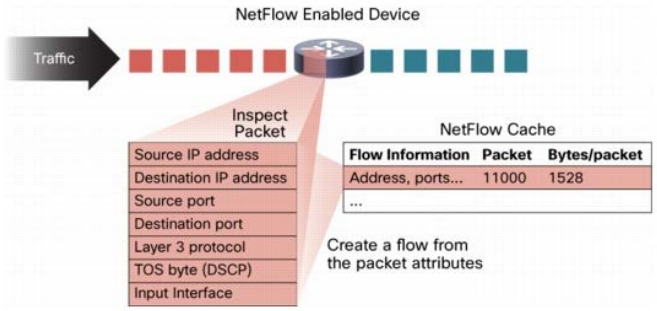

Fig. 2 Traffic flow in the NetFlow cache

To Implement NetFlow in the Network is typically used on a central site because all traffic from the remote sites is characterized and will be available within NetFlow. The location where NetFlow is deployed may depend on the location of the reporting solution and the topology of the network. If the reporting collection server is centrally located, then implementing NetFlow close to the reporting collector server is optimal. NetFlow can also be enabled at remote branch locations with the understanding that the export data will utilize bandwidth. About 1-5% of the switched traffic is used for export to the collection server.

III. NETWORK MONITORING PROCESS

The network performance is monitor using by analysis parameters of SNMP-MIB and NetFlow to find anomalous data flow and modify the network. This research is an experiment in the communication organization of Thailand that confront a problem of the network utilize on high traffic. The infrastructure of the communication organization network is shown in Fig. 3.

A. The problem of network monitoring

Nowadays, the network monitoring tools, PRTG, is show data flow with graph of traffic as shown in Fig. 4. Only data flow can be analyzed but it is not sufficient for solving the network problems.

B. Collecting Data of SNMP-MIB

The network administrator installs Solarwinds on PC for detecting data on router and must set SNMP Community string on Solarwinds to be the same as one on the router. Then, the important parameters of communication on the router are selected, which includes system, interface, route table, TCP and UDP connection as shown in Fig. 5.

C. Collecting Data of NetFlow

Collected NetFlow data provides useful information to analyze and to solve the network problems. The network in Fig. 3 is setup server with NetFlow Analysis to collect NetFlow parameters on the routers. The location of server is a central site and close to the server farm and internet for collecting data flow from user that access to data center. The router is configured in an interface for sending NetFlow to save on the server. The NetFlow data that occurred in database of conversation for finding parameters that is anomalous utilize traffic shown in Fig. 6. The table of NetFlow analysis show is characteristics of data flow such as Source IP, Destination IP, Application, Port, Protocol, DSCP and Traffic.

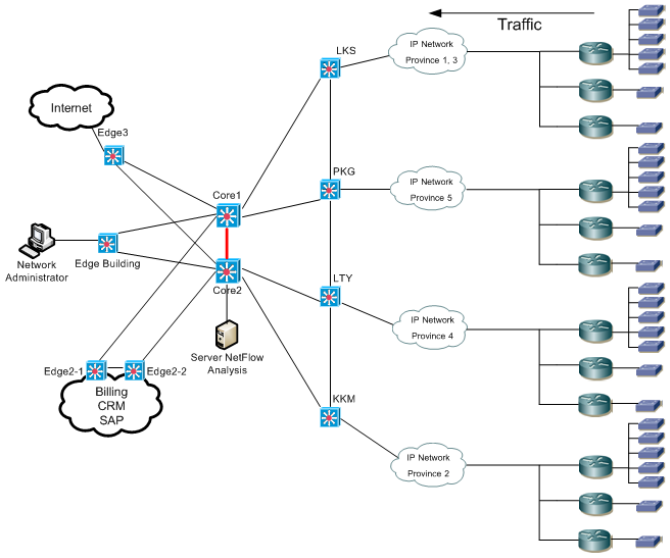

Fig. 3 Infrastructure of the communication organizations

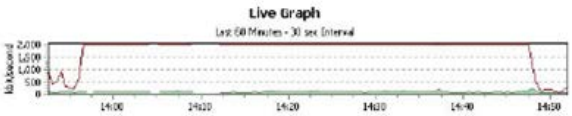

Fig. 4 Graph of the anomalies network traffic with PRTG

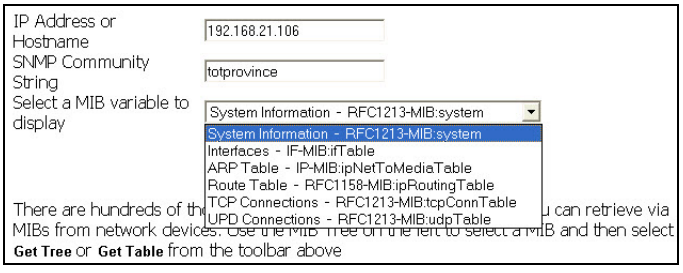

Fig. 5 detect accuracy connection on router with SNMP-MIB

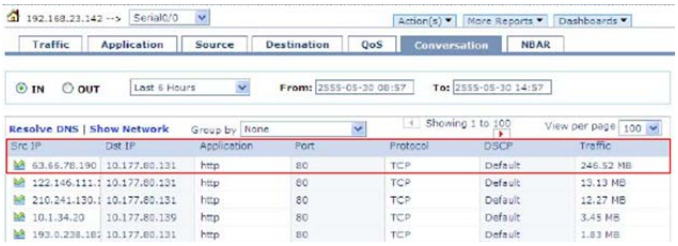

Fig.6 Tables of conversation on router

IV. ANALYSIS AND SOLVING PROBLEM

A. Analysis

First, SNMP-MIB parameters are considered such as system, interface, route table, TCP connection and UDP connection which can describe the status of the router as following details.

- *System*

Information about router as uptime-downtime, capability identified and location is described.

- *Interface*

For identifying the "superior" and "subordinate" is shown in each interface status.

- *Router Table*

Displaying multi-path routes and varying routes on network.

- *TCP Connection*

Information about current TCP connection by informing in the table that is transient and it ceases to exist when the connection makes the transition with no error occurred.

- *UDP Connection*

Local IP address and local port number for this UDP listener is shown. In the case of a UDP listener, any IP interface associated is meeting with UDP 161 only.

Second, data flow that shows traffic latency on router with NetFlow Analysis is monitored. This data shows an anomaly of the network such that IP: 10.177.80.131 refer to IP: 63.66.78.190 with an http application which is TCP protocol using port: 80 and receiving 246.52 Megabytes traffic. Note that, this size of data in communication is very large. The 246.52 megabytes transmitting data is equivalent to the book stacked high as two meters. This very big size of data is transmitting in 2Mb bandwidth channel and causes in performance degradation with reservation bandwidth. After considering all parameters from both SNMP and NetFlow, the problem can be identified to the user who downloads this very large size data from the network.

B. Solving Problem

When the problem that occurs by using large bandwidth in the network is found, to improve network performance and reduce effect of traffic latency can be solved step by step as following:

1st Step: looking for the problem user in database by searching IP: 10.177.80.131 is shown in Fig. 7.

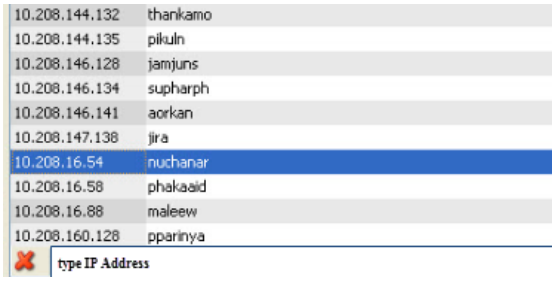

Fig. 7 Find IP of user on database

2nd Step: The behavior of access application by this user is examined.

3rd Step: Shaping this user bandwidth to 100Kbps on the bandwidth allocation of the organization is shown in Fig. 8.

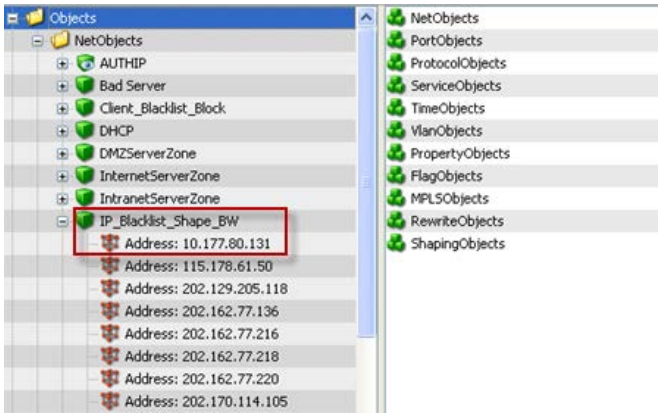

Fig. 8 Shape Bandwidth of user on bandwidth allocation of the organization

4th Step: Using NetFlow Analysis to review traffic values and looking for effect after shaping the bandwidth is shown in Fig. 9.

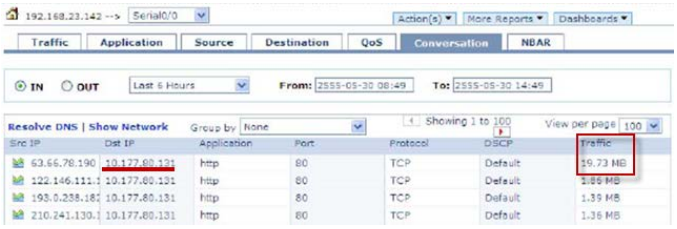

Fig. 9 Table conversation of NetFlow occur from effect of the shape bandwidth

In Fig.9, the very large traffic is reducing from 246.52 megabytes to 19.73 megabytes and this shows the efficiency of the shaping bandwidth method.

V. CONCLUSION

The SNMP-MIB parameters collected from Viewer Solarwinds software is experimented in a big communication organization in Thailand. These parameters can use for indicating the efficiency of router equipment. The other important parameters such as source IP, destination IP, protocol type, port number, and traffic utilization, is collected via NetFlow Analyzer. Then the software management can monitor and solve problem from the connection oriented and connectionless protocol traffic on the network. These parameters can be used to analysis the network security risk from attacker as well. This research should be benefit for the network administrator who requires analyzing method for their organization network.

ACKNOWLEDGMENT

I would like to express my sincere thanks to my advisor, Asst. Prof. Dr. Suwat Pattaramalai for his invaluable help and constant encouragement throughout the research. In addition, I thanks to my header, Mr. Noppadol boonrawdfor for assistance in the Infrastructure network and Mr. Suarpong wongchamchang providing the NetFlow Analysis and Solawinds tools. Finally, I most gratefully my parents and my friends for support throughout the period of this research.

REFERENCES

[1] http://kampol.htc.ac.th/web1/subject/com_network/sheet/sniffer_etherea l.htm.
[2] P. Barlet-Ros, G.Iannaccone, J. Sanjuas-Cuxart and J. Sole-Pareta "Predictive Resource Management of Multiple Monitoring Applications," *Networking, IEEE/ACM Transactions*, Vol.19, pp. 788-801, 2011.
[3] W. Zhang J. Gong, W. Gu and S. Cai "NetFlow-based network traffic monitoring," *Network Operations and Management Symposium (APNOMS), Asia-Pacific*, 21-23 Sept 2011, pp. 1-4.
[4] http://nfdump.sourceforge.net/.
[5] F. Zhu "NetFlow Data Acquisition Programming Design Based on Linux," *Intelligent Systems and Applications (ISA), 2011 3rd International Workshop*, May 2011, pp. 1-4.
[6] F. Strohmeier, P. Dorfinger and B. Trammell "Network performance evaluation based on flow data," *Wireless Communications and Mobile Computing Conference (IWCMC)*, 2011 7th International, July 2011, pp. 1585-1589.
[7] http://www.msit.mut.ac.th/newweb/phpfile/show.php?Qid=5310.
[8] http://www.manageengine.com/products/netflow/index1.html.
[9] http://scrutinizerthailand.blogspot.com/2010/05/netflow-sflow.html.