

Development of Mobile Network Monitoring System Fast Responsive Action On Network And System (mFRANS)

Istas Pratomo, Achmad Affandi, Dhany Riyanto

Department of Electrical Engineering

Institute of Technology Sepuluh Nopember (ITS)

Surabaya, Indonesia

istaspra@ee.its.ac.id, affandi@ee.its.ac.id, dhany13@mhs.ee.its.ac.id

Abstract—The increasing number of traffic on the network, due to the growth of smart devices such as gadgets and internet service at this time, causing high load of traffic. The network management is needed to find out the availability of the service, the network conditions, uptime and downtime. Simple Network Management Protocol (SNMP) is a protocol that is designed to monitor and set up a network based on TCP / IP either remotely or in a control center only. Through SNMP produce monitoring data in the form of raw data in the form of text, then the required application intermediaries to make the process monitoring be more efficient. This research will be to design, manufacture and testing the monitoring of all interfaces that exist on agent monitoring system that is more optimal. The experiment is conducted to determine the availability of devices and system using several methods, ie; on applications, network traffic and agent mapping, traffic in traffic out, polling system, urgent notification in the form text message and local alarm when detect the agent status up and down. The result of this study is a monitoring system that can provide a response notification to admin when there is agent down in the form text message with an average time of 22 to 30 seconds when the monitoring system detects the agent down and also traffic usage mapping, memory usage and availability.

Keywords; *SNMP, MIB, Manager, Agent, Availability, Sms Gateway*

I. INTRODUCTION

In today's digital era with the development of various types of gadgets causes the growth of traffic and the number of internet service on the network. To provide the maximum monitoring system that can determine service availability, network conditions, uptime and downtime. Monitoring network is one of the functions of the management system is useful to analyze whether the network is still sufficient feasible to use or need additional capacity. The monitoring results can also helpful if the admin wants to redesign the existing network. Lot of things in the network that can be monitored, one of which network traffic load via a router, switch interface.

Simple network management protocol (SNMP) is a protocol that widely used for network monitoring. A SNMP consisting of network management station (NMS) or SNMP manager and agent. Instead of traffic load in the network, other network conditions such as up or down status of a network monitoring device must be also monitored. Unlike the TCP with the ACK processes, the SNMP works on the UDP transport layer so that do not cause the traffic overload . Even though SNMP uses UDP transport that not cause overload the network because of the lack of the acknowledgment (ACK), but the process of monitoring itself may still cause traffic load on the monitored network. This is because the large number of information requests and responses between the manager and agent that impose the network.

Due to the use of SNMP protocol generates monitoring data in the form raw data, it is necessary to use intermediaries applications to quick reporting to the administrator when downtime occurs. so in order to make process monitoring become more efficient with the appearance of the graph [5]. In this research will design, manufacture and testing the technique for all interfaces that exist on the agent to make monitoring system more optimal. In this research NMS created with the interface form a website with support a database, network mapping and early warning systems (urgent notification) such as text message. The monitoring system done with the monitoring the campus ITS devices such as routers and switches. The experiment is conducted to determine the availability of devices and system using several methods, ie; on applications, network mapping, traffic TCP, polling system and text messages notification. The results of this research is an application that can explore the devices in the network, monitor the TCP traffic activities and the availability of each device that can send warning text message to the administrator when devices are down.

II. PREVIOUS WORK

In previous studies, the integration of SNMP with the database [1], an early warning system [2], network mapping [3], a PHP-based applications [4], and the fourth system monitoring process are still running separately. The next improvements performed on [5] with the incorporation systems that existed before, thus the function of monitoring process are more complete. In [5] simulated the process of monitoring conducted at the interfaces on each agent on the network so the

availability of services are monitored only one existing agent interface.

Whereas in [6] [7] [8] conduct research studies of the reduction of amount of packets monitoring a message between manager and agent in order to reduced load traffic when the monitoring process. The reduced amount of packets monitoring SNMP message was tested by group polling, where the number of agents are divided into groups and conducted by The IP multicast to each group [6]. Due to the use of a multicast system package delivery, the packet monitoring in group polling method send smaller packets between manager and agent. The weaknesses happened when the increasing number of agents causes delay and the amount of polling will also increase.

At [7], traffic load reduction on monitoring process conducted by modify the structure of SNMP message and the SNMP PDU. SNMP PDU contains variable bindings start time, end time, time intervals and sending time. The objective is to calculate the duration of the interval agent to get the requested information and also reduce the size of PDU SNMP to 21 bytes, thus reducing the load traffic with the faster response time. But it did not test the packet message reduction between manager and agent, thus the possibility of weighed the network process may be still happening. In [8], traffic load reduction on monitoring process conducted by the utilization assistance on NMS database is created to store frequently requested information by manager. Whereas the disadvantages of the standardization database and the efficiency database realtime testing are not performed.

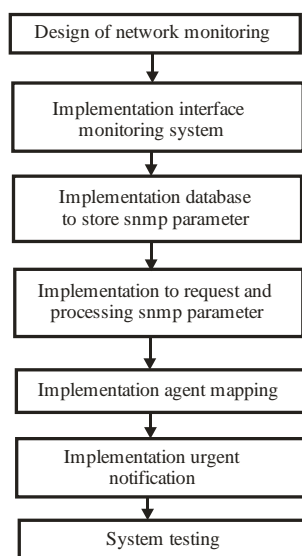


Fig. 1. Research step flowchart

I. MONITORING SYSTEM DESIGN

This research implemented an integrating of monitoring system that consists of network mapping, database, web interface and early warning system such as alarms and sms. On the design stage, we determined the parameters of SNMP MIB agent on all interfaces to be retrieved and processed

monitoring system such as TCP traffic, Up and Down device status, the memory usage, and reduction systems process package to bandwidth optimization. The methodology of our research flowchart is presents in Figure 1.

A. Implementation System

We have designed an SNMP monitoring system as shown on Figure 2 below. It consists of interface, web server, database, PHP, SNMP and mobile devices. The manager is connected to user and network.

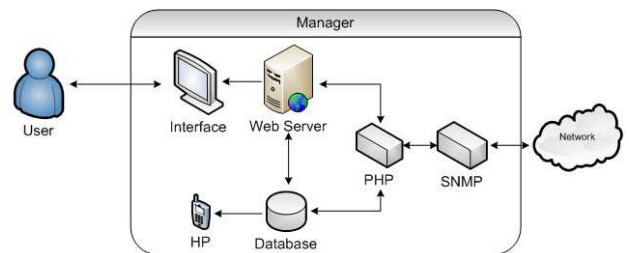


Fig. 2. General overview system

B. Interface, Polling and Database Module

The implementation of interfaces and polling module are conducted using open NMS Cacti version 0.8.8b by version 1.8.3 XAMP database consisting of PHP 5.5.11 Apache 2.4.9 and phpMyAdmin 1.4.12. The objective of implementations web interface is to display the process of monitoring results, whether already or is being done.

C. Agent Mapping Module

The implementations of these modules are aims to find agents that are connected between the manager, relation between agent and the traffic conditions in the form graphs in realtime. When the polling process occurs, based agent that already exist on the list, the traffic conditions on the interface will be saving in the database. So the network condition between agent can be drawn on the network map that was made before.

D. Urgent Notification Module

The aims of implementation Urgent Notification module is to provide emergency notification text message to the admin in case of downtime and uptime. This system works simultaneously with polling system. When the results of agent states in down or up conditions, the text message will be sent to admin with the format time, agent notice, and agent states. SMS gateway module implementation are conducted using Prolink GSM modem connected via computer USB port monitoring server and the sms gateway software used is Gammu.

E. Monitored Agent Mapping

The monitoring system is conducted in campus ITS networks. Figure 3 shows the architecture of monitoring devices system that monitored :

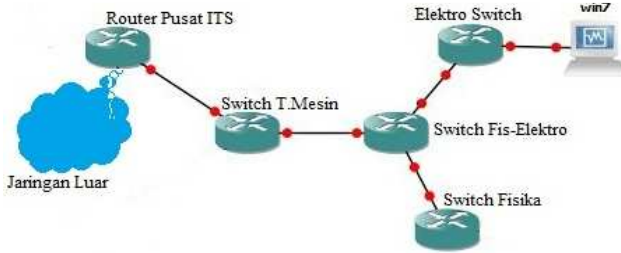


Fig. 3. ITS system architecture

II. TEST AND RESULTS ANALYSIS

The implementation of monitoring system is conducted to examine the success level of web interface and functions interface to operate the monitoring system. Firstly, the user must enter the username and password as an admin. After the login process is successful, the application can be executed. The first process we must add devices that monitored with the ip device SNMP feature is activated so polling process can be excute every five minutes. The process taken value of TCP traffic agents is illustrated in figure 4 and 5, status and availability device are shown in figure 6. At the polling process is running, the manager will requesting all of the information that will be monitored by the existing oid the MIB of each agent and will store the information to database manager that will be displayed in the admin web monitoring and network mapping system. Of all the agents that monitored interfaces, bandwidth optimization process can be applied to see which agent that use tcp and udp traffic with high bandwidth, so with this information the administrators can determine a more appropriate allocation of bandwidth for each network.

In the form of the application monitoring system, the main part of web interface consists of:

1. Console : The menu console are used to
 - Setting the implementation of monitoring system in monitored devices.
 - Management generated graphs.
 - Monitored data sources.
 - Data collection methods.
 - Monitored graphs template.
 - Type of the polling is used.
 - Export graphics.
 - Device status.
 - IP and avalability.
2. Graph : The menu are consists the monitoring graphs results of all features such as filter time zooming and export traffic to excel data.

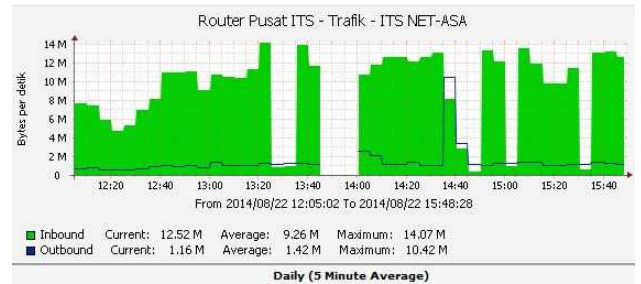


Fig. 4. TCP Inbound agent traffic

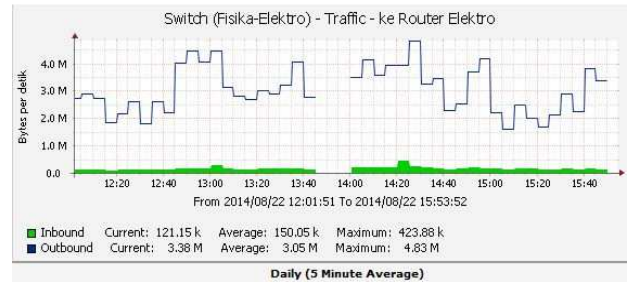


Fig. 5. TCP Outbound agent traffic

Description**	Hostname	Status	Availability
Elektro Switch	10.122.100.100	Up	89.66
JTE-A	10.122.100.100	Up	89.53
Router Pusat ITS	10.11.100.100	Up	90.7
Switch (Fisika-Elektro)	10.20.100.100	Up	90.59
Switch Fisika	10.11.100.100	Up	90.59
Win7	localhost	Up	100

Fig. 6. Name, IP, state and availability

On the monitoring system using two types of polls are CMD and Spine, where the purpose of the testing system of this poll is to determine how long the completion of the single monitoring server polling with polling period every five minutes. Number of polling examined, ie five times the poll with comparison of the agent versus time. Figure 7 below is a polling system test results are used.

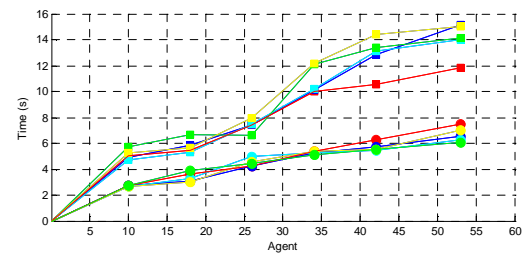


Fig. 7. CMD and Spine system polling result

Picture Description :
Symbol ● : Polling Spine
Symbol ■ : Polling CMD

Based on polling data that has been plotted with five times the poll testing, it appears that polling by using the spine poller faster than the poller CMD. This is because the spine poller has the ability requesting greater amount of OID on a request packet. Whereas poller CMD can only requesting one OID in one package request. Appears that with difference poller used in monitoring systems greatly affect the time required by the monitoring system to obtain data. Where the difference between the poller CMD with Spine the more devices that monitored the longer poller CMD to obtain data. Where the difference between the poller obtained from the time difference between the use of polling CMD and Spine, the longer polling process is completed or the greater the difference time it will affect the length of text message notification received. This is because the process of sending text message notification starts after the polling process completed.

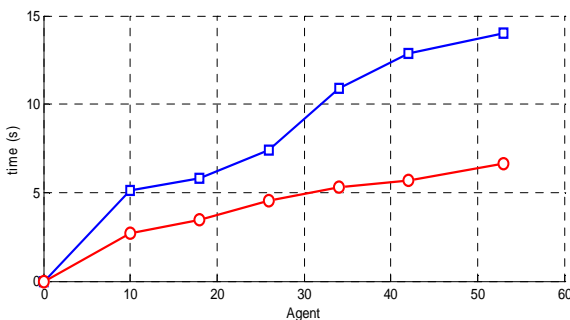


Fig. 8. CMD and Spine system polling average

The mapping system that monitored agent described by the connection of the agents, where each link of the agent constitute the agent interface usage bandwidth in realtime. With this system would make easier administrators to optimize the bandwidth used. Figure 9 below is a topology obtained from the mapping monitored devices.

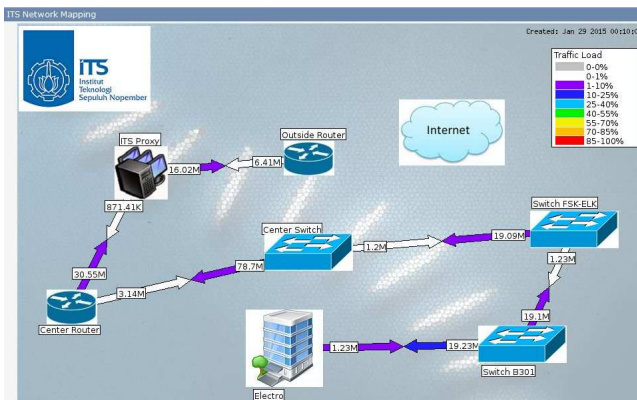


Fig. 9. Agent mapping system

The early warning system indicate icon condition of each agent, which is marked with a green icon for up status, red icon for down status and blue icon for recovering status. The monitoring system will provide alarm alerts when detecting agent down. Figure 10 below show the agents monitor status of the monitoring system.

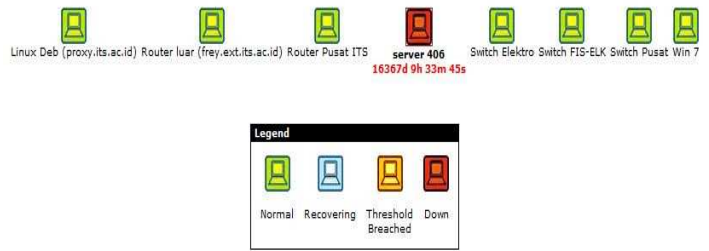


Fig. 10. Status monitored agent

When monitoring server detecting agent down or up status while polling process occur, the server will send text message to admin. Figure 11 below show text message to admin when detecting agent down or up status.

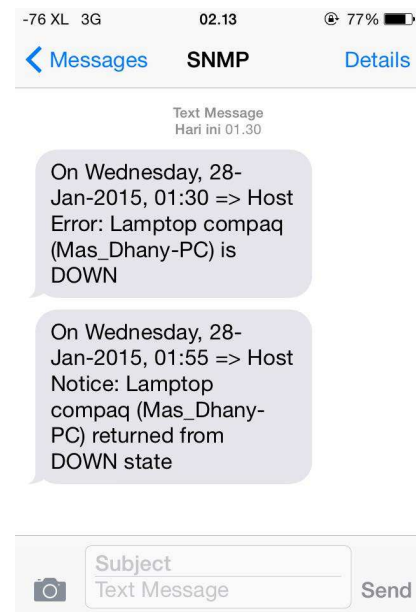


Fig. 11. Text message to admin

In the aspect SNMP protocol security, this research use SNMP version one and version two, where is this security version using name that is set in the agent community. For the future research, in terms to improve the security monitoring system could use SNMP version three where is this security version using the agent community, username and password with sha or md5 encryption so that the monitoring process becomes more secure. Also SMS testing with different cellular operators in terms to determine sms delay of each operator.

III. CONCLUSION

From the application server monitoring system that has been implemented and tested, the conclusions can be drawn as follows:

1. The utilization of SNMP protocol for monitoring system can provides optimal results and can be used to monitor network device that support SNMP.

2. Protocol SNMP works by request the value of parameter based on the OID which can perform its functions.
3. The text data raw generated by SNMP monitoring made the web interfaces more easily to the analysis the results.
4. The agent with condition down if : monitored device is damaged or down, the connection problems or not connected, the interface or agent unreachable because it does not suport snmp.
5. Monitoring server applications can perform realtime monitoring, provide information of the problems that occur and send sms to admin if the agent status change to down or up so the administrator can quickly handle the problems.
6. Availability have heavily influenced on the uptime and downtime of devices. The longer uptime of a device cause the availability value more greater.
7. Monitoring system that can provide a response notification to admin when there is agent down in the form text message with an average time of 22 to 30 seconds when the monitoring system detects the agent down.
8. The use of spine polling system can accelerate the process of getting data due spine poller has the ability requesting greater amount of OID on a request packet. Whereas CMD poller can only be requesting an OID on a request packet.

REFERENCES

- [1] Reza Pradikta "Rancang Bangun Aplikasi Monitoring Jaringan Dengan Menggunakan Protokol SNMP (Simple Network Management Protocol)", JURNAL TEKNIK POMITS, vol. 2, No. 1, ISSN 2337-3539, 2013
- [2] Ayu Hidayatul Romadhani "Sistem Peringatan Dini pada Operasional Jaringan Berbasis Network Monitoring", Jurnal Teknik Pomits, vol. 2, No. 1, ISSN: 2337-3539, 2013
- [3] Vincentius Bima Anong Dian Hutama "Rancang Bangun Network Mapping Sistem Monitoring Jaringan.", Jurnal Teknik Pomits, vol. 2, No. 1, ISSN: 23373539, 2013
- [4] Sri Puji Utami A., Surya Agustian, Iman Fauzi Aditya Sayogo "Perancangan Online Network Monitoring Berbasis PHP dan SNMP", Seminar Nasional Aplikasi Teknologi Informasi, ISSN: 1907-5022, 2006
- [5] Muazam Nugroho, "Rancang Bangun Aplikasi Monitoring Jaringan Menggunakan SNMP (Simple Network Management Protocol) dengan Sistem Peringatan Dini dan Mapping Jaringan", Jurnal Teknik Pomits, vol. 3, No.1, ISSN: 2337-3539, 2014
- [6] Kyo-Cheul Hwang, Jong-Joon Hong and Kyoon-Ha Lee "A SNMP Group Polling for the Management Traffic", Dept. of Computer Science and Engineering TENCON (IEEE) Journal, vol. 99, pp. 0-7803-5739-6, 1999
- [7] Chunkyun Youn, "A study for decrease of SNMP messages through an efficient processing of trend analysis information", Dept. of Internet contents ICTC (IEEE) Journal, vol. 12, pp. 978-1-4673-4828-7, 2012
- [8] Omar Said, "A Novel Technique for SNMP Bandwidth Reduction:Simulation and Evaluation", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.2, February 2008
- [9] Diana Chase, Barbara Daniell and Judith Sherwood Universal Server: SNMP Subagent Guide, INFORMIX: California, March 1997.
- [10] Syamsudin M "60 Menit Belajar Sistem Monitoring (Cacti)", Computer Networks Singapore, 2008
- [11] ITIL "How to Develop, Implement and Enforce ITIL v3 Best Practice.", The Art of Service, Brisbane, 2008
- [12] Ian Berry, Tony Roman, Larry Adams, J.P. Pasnak, Jimmy Conner, Reinhard Scheck and Andreas Braun, (2012), "The Cacti Manual", The CactiGroup. (accessed by 22 August 2014).
- [13] Information Sciences Institute "Transmission Control Protocol,", RFC 793, University of Southern California, September, 1981
- [14] Borman, D "TCP Options and Maximum Segment Size (MSS)", RFC 6691, IETF, Juli 2012
- [15] J. Postel "User Datagram Protocol,", RFC 768, ISI, 28 August 1980