DESIGN AND IMPLEMENTATION OF REAL-TIME MRTG++

Namkyoung Um*, Chungsik Oh*°, Sangho Lee*

Dept. Computer Science, Chungbuk National University*, family@netsec.cbnu.ac.kr
KISTI*°, ocs@kisti.re.kr

ABSTRACT:

We design as well as implement MRTG++ enhanced by eliminating drawbacks of original MRTG. Existing MRTG makes it easy to monitor network resources on the web, and it can show some trend utilization about resources of remote systems. However MRTG has only functions showing statistical information data with daily/monthly/yearly characteristics in real-time, and periodically deletes stored data. Thus we improve log file-based storing method as an effectivelly storing method with database, propose expended MRTG++ retrieving as well as managing with measured data. It also can be applied in ubiquitous environment..

KEY WORDS: MRTG, SNMP, Network Monitoring, Network Management

1. INTRODUCTION

As the quantitative expansion and qualitative growth of Internet services, problems such like the increase in user data and the bottleneck state of networks have been occurred. In order to solve these kinds of problems, it is necessary to build the environment not only monitoring and analysing the usage of network resources, but also deploying restricted resources on networks effectively. In general, there is a freeware such as MRTG (Multi Router Traffic Grapher), which can be used as a typical program to monitor network systems and measure traffic gotten by access to remote systems. MRTG routinely displays the result as HTML format after generating either GIF format or PNG format from the amount of the results monitored every designated time, so it is easy to observe them. However, there are two drawbacks on the system; one of them is that original MRTG has only the function displaying statistical information data in real-time per date/month/year and the other one is the fact not to have recycling effects because stored data is deleted periodically. Thus we propose MRTG++ enhanced with the functions such as powerfully displaying GUI and recycling points. To compare with existing MRTG, MRTG++ has the advantages like the following; firstly, the existing MRTG used to periodically delete data stored as log-file format, MRTG++, on the other hand, has database for storing measured data and also changes the period which means either storage or deletion time of data. Secondly, we will expand existing MRTG as web-based monitoring program for network resources by using the functions, that is, searching status of network resources as well as analysing them at a look[1][2][3].

In this paper, chapter 2 describes related works in the field of network management system and monitoring system. Chapter 3 provides MRTG++ monitoring system with global architecture and each module in the system. Chapter 4 implements the system designed in chapter 3 and evaluates it with any other similar systems to MRTG. Lastly, chapter 5 describes conclusion and future works.

2. RELATED WORK

2.1 Previous MRTG system

There are two kinds of approaches to network analysis, which are Active and Passive approaches according to methods collecting and analysing either any devices on networks or information about any traffics. The former is managed by using test packets sent to the monitored devices, on the other hand, the latter is analysed through data stored on collective devices. MRTG belongs to the latter. As the existing similar tools, there are RRD, Cricket [7] and so on. The features of MRTG is like these:

- It operates on most of Unix systems and Windows NT.
- As the unique algorithm to arrange log-file is adapted, the size of log-file in MRTG is not allowed to be bigger.
- It programmed the part of SNMP by using Perl available for portability, so we don't need to install extra SNMP packages.
- MRTG automatically notices to network managers when the configuration of router ports is changed.

As seen in Fig.1, MRTG supports GUI (Graphical User Interface) displaying as HTML format. It's a type of open source to monitor traffics on network devices. Fig 2 shows operation of MRTG. During the operation, MRTG uses SNMP (Simple Network Management Protocol) for alerting abnormal symptoms, also.

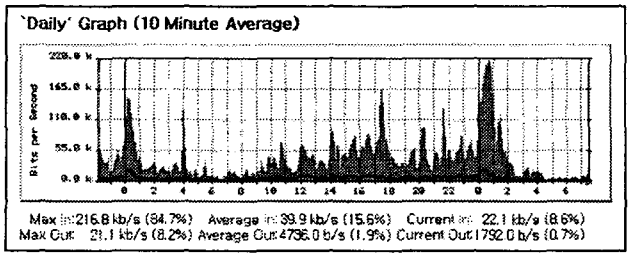

Figure 1. The graph of MRTG

2.2 Operation of MRTG

The principles on MRTG operation are the following; SNMP collects network related information on devices connected to networks and then alerts the things to a manager. SNMP is a kind of protocol to manage networks like Internet. It operates as a server-client based model, and manages agents, for example, the network nodes or devices, and a manager. The manager manages the information as a centralized manager. Fig. 2 illustrates the operation of MRTG.

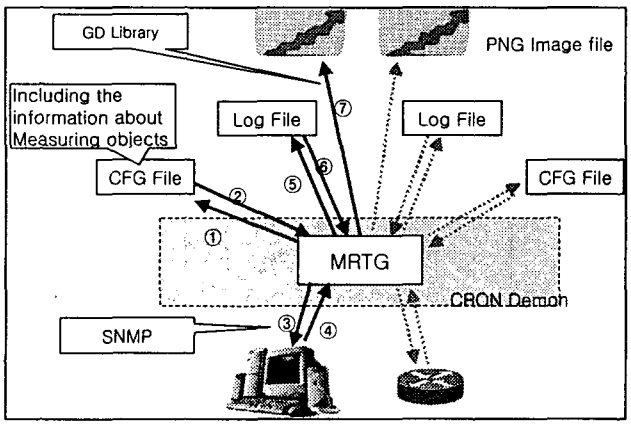

Figure 2. Operation of MRTG

The order for operation is the following:

1. MRTG shows traffic trend by using PNG image format through measurement of the traffic load on networks.
2. It generates log-file taken by question and answer method via MIB (Management Information Base), which is taken by measured objects, of SNMP (Simple Network Management Protocol).
3. It shows web based real-time traffic trend by using traffic information collected through routers or switches.

2.3 Interoperability between MRTG and SNMP

It is no need to keep connecting constantly for SNMP because it normally uses UDP (User Datagram Protocol) as a transmission protocol. Thus the system has advantages such like the fact it doesn't use resources much, on the other hand, it has a problem that the reliability between agents and managers is not guaranteed. Besides, it is basic to both give and take specific information between the agents and the managers. In SNMPv1, there are four kinds of functions, that is, *Get, GetNext, Set, Trap*. It will show in Fig. 7[3][4].

3. MRTG++ MONITORING SYSTEM

3.1 Consideration for designing this system

MRTG++ we design in this paper is basically following passive approach in the network analysis method, and this is a way to perform a variety of performance of network devices and store the data[5][6].

Overall, this system consists of four functional modules and DBMS. These are like following:

- *Administrator module* has web based system management
- *Viewer module* shows usage trend on web
- *Information management module* is designed as storing usage trend in database directly
- *Information collection module* designs it via interoperability between Perl and MySQL.
- *DBMS* uses MySQL DBMS

The structure of MRTG++ is like in Fig.3

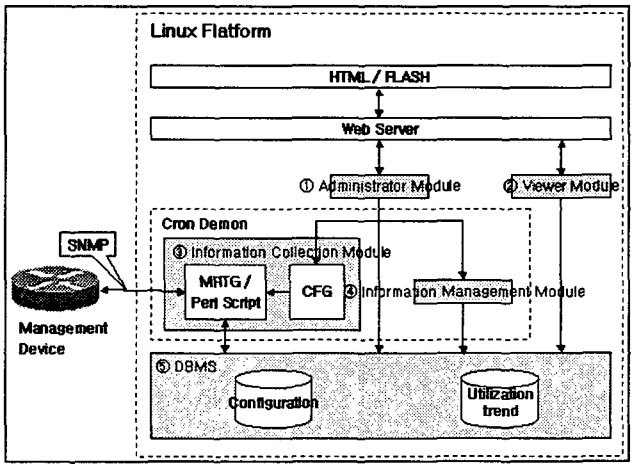

Figure 3. Structure of MRTG++

The trends for devices of managed objects are showed by means of total lists and detailed items and the detailed items are Ethernet card, IP, CPU, Disk/Memory/Swap capabilities and community name which means the network domain to be managed.

Fig 4 and Fig 5, respectively, have the functions of an administrator module and viewer module. The administrator module manages total devices on the network, whereas the viewer module is the part of showing usage trends of system conclusively.

Fig. 4 is an administrator module and Fig.5 is a viewer module in MRTG++.

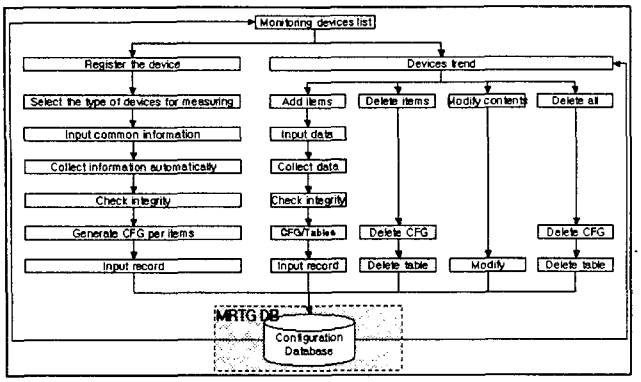

Figure 4. Administrator Module

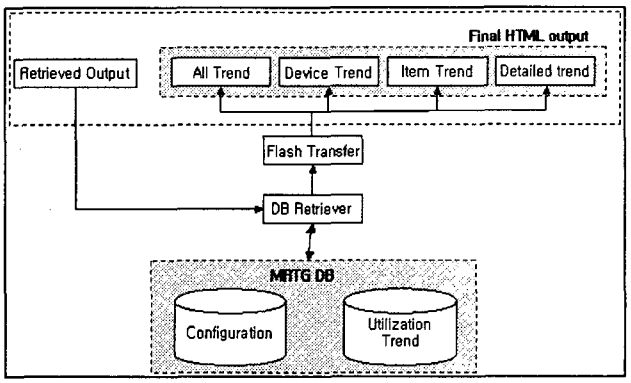

Figure 5. Viewer Module

Fig. 6 is an information collection module and Fig. 7 is an information management module. The information collection module is to collect the status of measured resources by taking set-up information of CFG files and to store the information in database conclusively. Also it collects data from network via interoperability between SNMP and it.

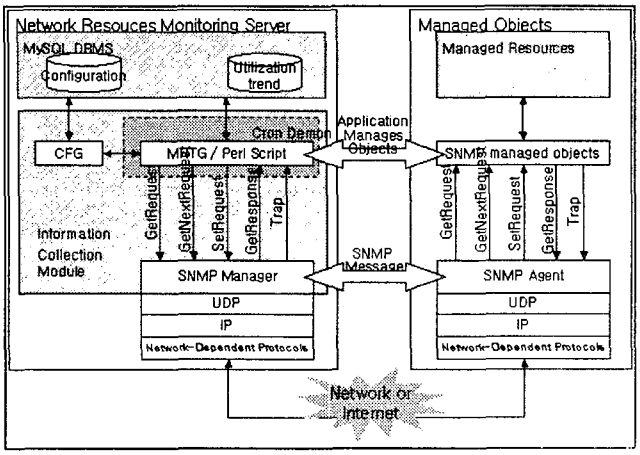

Figure 6. Information Collection Module

The information management module automatically manages tables for utilization trend according to set-up information of configuration tables and not only supports the function for translation of averages about the trend but also deletes database records by limited storage period and backup function as well.

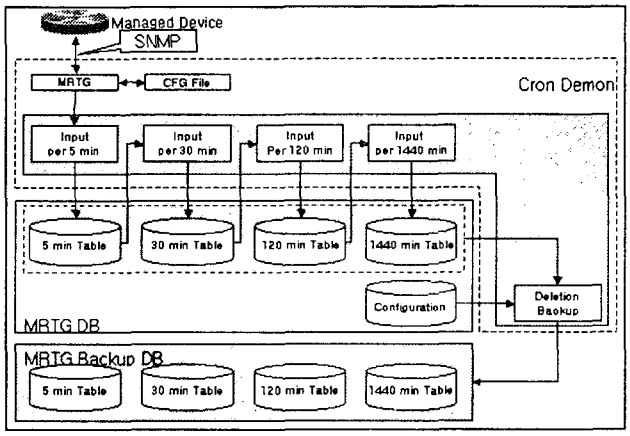

Figure 7. Information Management Module

4. IMPLEMENTATION AND EVALUATION

4.1 System environment

To build MRTG++, the information collection module is developed by making up Perl of MRTG-2.9.22 and SNMP tool to enable to use MRTG and PHP modules is used by UCD-SNMP-4.2.4.

4.2 Functional tests

The screen of the suggested system is like Fig.8. By expressing as Flash, if someone want to see detailed one, they can see the selected part as expanding. The following is the shortcut about real-time monitoring and retrieving.

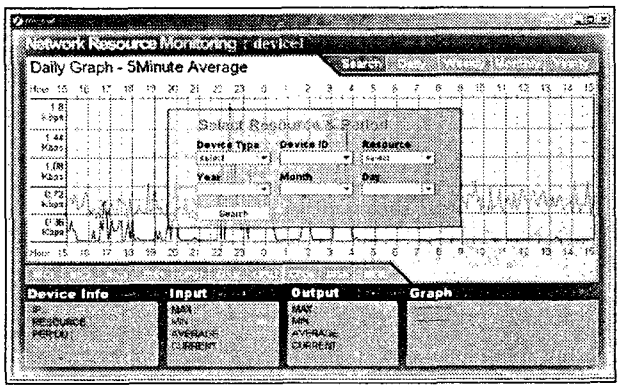

Figure 8. View of retrieval system in MRTG++

After measured, the data will be stored in tables per 5/20/120/1440min and it is automatically moved to other backup table when the data is overflowed.

4.3 Evaluation of this system

The features and advantages of this system is like following.

1. It is possible to either monitor or retrieve the results in real-time
2. It is possible to recycle the measured data
3. It is possible to manage capabilities of database effectively.
4. It is easy to use.
5. It has direct interface with users.
6. It is cheaper to develop than the other tools
7. It is excellent to expand as greater tool sufficiently.

As seen in Table.1, MRTG++ surpasses any other tools such as MRTG, RRD tools, and Crickets, overall.

Table 1. Evaluation via previous systems

Comparison items	MRTG	RRD	Cricket	MRTG++
Web-based interface	o	o	o	o
Real-time monitoring	o	o	o	o
Period/Device/Resources monitoring	Δ	Δ	Δ	o
Utilization trend search	×	×	×	o
Interactive design transformation	×	×	×	o
Cheap development cost	o	o	o	o
Collection of Resource status	o	×	o	o
Data conservation with DBMS	×	Δ	Δ	o
Treatment of database	×	×	×	o

5. CONCLUSION

We presented enhanced and expended network monitoring system from MRTG and designed MRTG++. Also we implemented it as actual interactive flash format and made it high through direct GUI. In this paper, we suggested algorithms for storing in database effectively.

In the near future, we will perform detailed analysis about monitoring data based on the new monitoring technologies and information management methods. Also as a result of the analysis, we will develop and research the direction to design fault management function and network configuration. Thus we should add a function for storing log-file in consideration of database capability, especially, in order to express the stored log-file as flash, formally we need to research algorithm for graphical way effectively.

6. REFERENCES

[1] Fred Halsall, 1990, "Data Communications, Computer Networks and Open Systems", Fourth Editon.

[2] K. McCloghrie and M. Rose, 1990, "Management Information Base for Network Management of TCP/IP-based Internets," RFC 1156

[3] William Stallings, 1999, "SNMP, SNMPv2, SNMPv3, and RMON 1 and 2", Addison Wesley

[4] J. Case, M. Fedor, M. Schoffstall, and J. Davin, 1990, "A Simple Network Management Protocol (SNMP)," RFC 1009

[5] Cisco Technology - Simple Network Management Protocol,http://www.cisco.com/warp/public/535/3.html.

[6] Tobias Oetiker, Dave Rand, MRTG : Multi Router Traffic Grapher, http://people.ee.ethz.ch/~oetiker/webtools/mrtg