

Automatic Event-Driven System for Network Management

Ya-Ling Wang, Arak Sae Yuan and Quincy Wu

Department of Computer Science and Information Engineering, National Chi Nan University, Taiwan

{s100321521, s99321058, solomon}@ncnu.edu.tw

Abstract— It is very tedious and trivial if a network administrator has to manage all the equipment manually. Unfortunately, there are usually numerous and heterogeneous devices over which an administrator must watch. This paper proposes the design and development of an automatic event-driven system to reduce the burden on network administrators. By allowing managers to pre-define the action of some conditions, the network management system can quickly respond to critical events and mitigate the network trouble, in contrary to many commercial network management systems which can only send a notification to administrators. For example, if a user tries to download 10 GBytes of files in a single day, which is a behaviour violating the acceptable user policy (AUP) in campus, it may be necessary to limit the bandwidth of the user in order to prevent the campus network from being jammed because of a single user. With our system, an administrator can easily configure the network management system to automatically take actions so that the managers need to do nothing to impose appropriate penalty on individual users. The system will control devices by Simple Network Management Protocol (SNMP), which is supported by most network devices such as routers and switches. In this paper, we implemented the system in our campus, and chose the switches as the device to control user behaviours. This system obtains information from devices by SYSLOG, while it sends instructions to devices through SNMP. In a real case we found that when a device breaks down, the system can solve the problem automatically and immediately take responses as defined by the manager. The manager will get the report by emails and MSN messages, too. In case of equipment upgrades where some devices will stop working temporarily, the manager can also modify the reaction through this system to prevent it from sending out false alarms. This system provides managers a convenient tool to handle abnormal situations in real-time monitoring.

Keywords—AWK, MSN notify, SNMP, Switch, Syslog

I. INTRODUCTION

For server administrators, it has always been a tedious but necessary duty to make sure their facilities work normally. Although servers can work favourably most of time, they can always have a big trouble suddenly. To ensure devices operation properly, manager may replace some unstable component in advance according to the expected working age of the equipment [1]. For example, the Central Trust of China (CTOC) suggestion vendors should provide at least one year warranty for a switch, and the switch manager can take the warranty time as a reference. Despite of the warranty devices

are still under some level of risk, so administrators have to closely monitor their hosts and check whether there is any symptom of accident.

Moreover, in addition to the large number of device, manager may supervise heterogeneous devices such as routers, LAN switches, WLAN Access Points (APs) or FTP servers, etc. For different services, usually managers need to configure them by different ways [2][3]. For instance, change a router configuration by telnet, reload the service on a FreeBSD server by secure shell (SSH), or restart a switch via the web interface. All these actions require the manager to have Internet access. If managers have no Internet access at the moment, they cannot respond to the problems quickly.

This paper proposes Automatic Event-Driven (hereinafter referred to as AED) system architecture to handle this problem by allowing managers to pre-define events. With SYSLOG [4] and Simple Network Management Protocol (SNMP) [5], which are supported by most network devices, the AED system can automatically solve pre-defined problems by itself. As shown in Figure 1, all devices send SYSLOG messages to the AED system. Managers can pre-define the reaction when some situation happens. The system will look for these abnormal conditions by parsing rules specified by the manager. Therefore, the system can recover from the abnormal situation through SNMP instructions.

One word for the design philosophy: Although messages can be collected either by SYSLOG or SNMP [6], the system will become much simpler and flexible if we use both of them. No matter the device is a router or a switch, the data will all be stored by SYSLOG while the AED system can control network devices through SNMP.

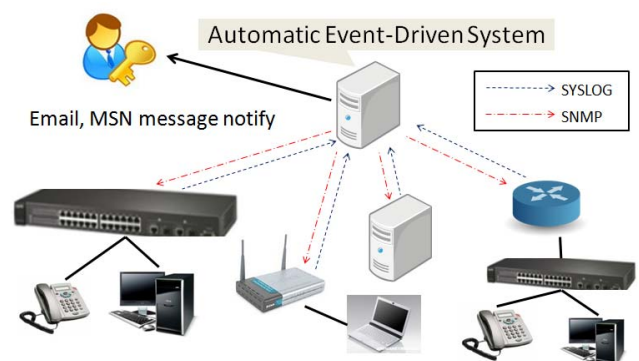


Figure 1. Event-driven system architecture

The AED system will also notify the server manager by emails and MSN instant messages after appropriate actions have been taken. This provides managers a bright way to be aware of how troubles are solved, even if they are incapable of accessing Internet when the devices break down.

II. RELATED TECHNOLOGIES

Three network management tools are used in the AED system. We use SYSLOG to collect the data, and SNMP to send instruction to devices. AWK scripts are utilized to parse the large amount of log files and match the conditions specified by managers.

A. Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is a widely used network management protocol. It has been adopted by numerous network equipments as a management interface. Figure 2 shows a basic diagram illustrating the SNMP operation.

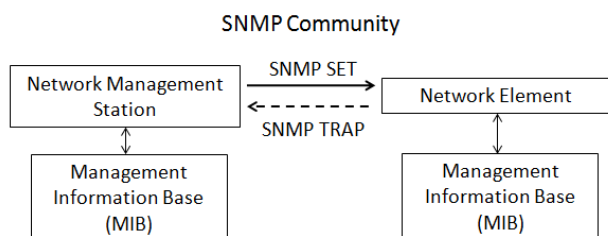


Figure 2. SNMP basic diagram

SNMP defines a client/server relationship. SNMP clients run on network devices. The network element shown in Figure 2 is the network device we want to manage. The network management station is the SNMP manager. The data controlled by the SNMP agent is SNMP Management Information Base (MIB). Through the MIB value, SNMP can monitor the status of each device easily [7]. Network Management Station can send instructions to a network element by *snmpset* commands while SNMP agents will use SNMP traps to provide abnormal alerts to servers [8]. The AED system use *snmpset* to send the instruction to network devices, but collect device information by SYSLOG instead of SNMP traps.

B. Syslog

Syslog is a standard for logging program message. It has been extended to a new version called **syslog-ng**, which is implemented as open source software for Unix systems. It provides devices a way to log important messages [9].

Figure 3 shows the distributed mode in the AED system. With **syslog-ng**, the log can be classified to different directories. The log coming from heterogeneous devices will be stored into different directories under */var/log/HOSTS*. For each device, they will use the *IP (Internet Protocol) address* as the directory name. Take a router for example, when there are more than one router, each router will store its log under

the directory with its IP address as the directory name. Finally, the data will be stored with the filename *date* for retrieval.

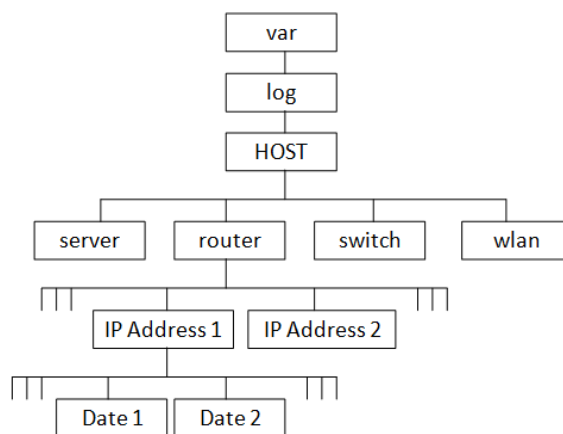


Figure 3. A sample directory tree of SYSLOG

C. AWK

The AWK is a data processing language. It can extract data to produce flexibly formatted reports. With the data-driven scripting language, it will take pre-defined actions through different options [10]. For example, if you want to print the second column of each line, where columns are separated with the character “:”, then you can use the command:

- `awk -F':' '{ print $2 }'`

The AED system uses the same idea of “patterns-and-actions”. With different options, the managers can pre-defined a variety of events for AED to handle automatically.

D. Instant Messaging

It is important to notify the administrator when there is something wrong on a server. Many traditional network management tools notify the administrator using emails. However, because email was not designed for real-time communication, it may take a long time for the administrator to get this notice after a server has stopped working. Therefore, it would be beneficial to notify the administrator with instant messaging services, such as Microsoft MSN Messenger. Suppose the administrators are online using MSN instant message services, they would be able to receive notifications in real-time, either on their smart phones or desktop computers. The AED system incorporates the MSN Robot to send out the notification via MSN.

III. ARCHITECTURE AND COMPONENTS

The implementation environment takes the dormitory network of National Chi Nan University (hereinafter referred to as NCNU) as an example. In each room there have two Ethernet ports for each student, one for a computer, and the other for a voice over IP (VoIP) phone. To make sure the data traffic of computers will not interfere with the voice traffic of IP phones, these two kinds of devices connect to different virtual LANs. Unfortunately, sometimes students may accidentally connect two RJ-45 ports with an Ethernet cable,

and form a loop as shown in Figure 4. This will generate large amount of packets which overload the CPU of the switches, and slow down the performance of the overall network.



Figure 4. The loop in the dormitory network

In order to avoid network loops accidentally made by students, two pre-defined events are identified in this prototype:

- 1) When a user plugs out his/her device from the switch port within ten minutes, the AED should notify the manager.
- 2) If a device was plugged into a switch port, the bandwidth of the port will be restricted to 128kbps only.

The bandwidth restriction can mitigate the impact of broadcast storm caused by the loop, while the manager can receive notifications to investigate what devices have been changed.

A. Architecture

We choose a layer-2 switch as the testing device. The AED system is running on a Linux CentOS 6.0 system. The architecture is shown in Figure 5. In the AED system, we will use SYSLOG to collect data, and use SNMP to send instructions to devices. With such large amount of data, we use AWK scripts to parse the log data in accordance with predefined rules.

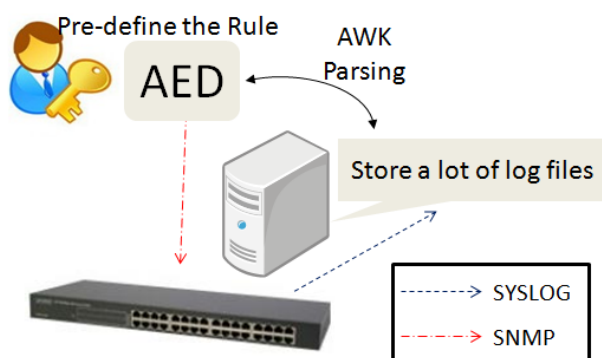


Figure 5. The AED system's operation

B. Parsing Options

For the AWK script parsing, we apply the “Action and Pattern” idea. According to different options, the script will execute different functions. The option list is shown in Table 1.

TABLE 1. PARSING OPTION

Option	Meaning	Value
-t	On a regular time	<Number>
-c	Connect to what kind of device	Switch
		Router
-o	What option should be parsed	Up
		Down
-i	Notify the manager	<Email>
-l	Limit bandwidth to Kbps	<Number>

The option list can certainly be extended, according to the features supported by the switches or routers. Here is a brief explanation of the above options:

1) **-t**: The administrator wants to execute this rule periodically. If you do not supply this option, the action will only be executed once.

2) **-c**: Specify what kind of device will be monitored by the AED system. At this moment two kinds of devices (layer-2 switches and layer-3 routers) are supported.

3) **-o**: Which keywords should the AED system search in the log files. There are a lot of ports on one switch. The “UP” message means the port has a device plugging in while the “DOWN” message means a device is plugged out of the port or the device is powered down.

4) **-i**: When an event happens, the AED system has to notify the administrator. Through this argument, different events can be configured to be sent to different administrators.

5) **-l**: Each port on the switch can be configured with an upper limit of transmission rate. This option can flexibly adjust the target device for different requirements.

The value for -t and -l are numeric numbers, and the value for -i are the email address of the administrator.

C. Specifying the rules

For example, if an administrator wants to define an event, he/she should use the format as below:

1) **AED -t 10 -c switch -o DOWN -i root@localhost**

2) **AED -t 20 -c switch -o UP -l 128**

As shown in Figure 6, if the administrator wants to execute the program every five minutes, the system can be invoked using option -t to modify **crontab**. Because SYSLOG will classify different types of log data into different directories, with the type of the device, we can know which log file we should look for, and use the option -o to extract the UP/DOWN status of the target device. After analysing the log file, the AED system can accordingly send SNMP requests, to

perform some tasks such as bandwidth limiting. Finally, the AED system will use notify module to send a warning to the administrator.

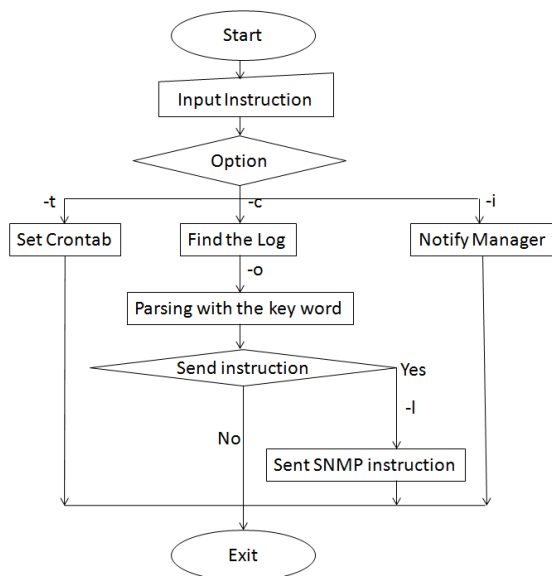


Figure 6. Flow chart of option parsing

In Figure 6, it can be seen that some events may have impact on others, such as `-c` and `-o`. For those events that will send out SNMP commands, the instruction must include the `-c` and `-o` option. This restriction is intuitive. If the AED system has not parsed the log data, it could not send out instructions to turn on/off the target devices.

D. Sending message

There are a lot of tools which allow developers to send messages via the MSN service. We choose the **sendMsg** [11] software package. The **sendMsg** is a PHP class which allows users sending messages to a contact from a specified account. The flowchart of sending messages is shown as Figure 7.

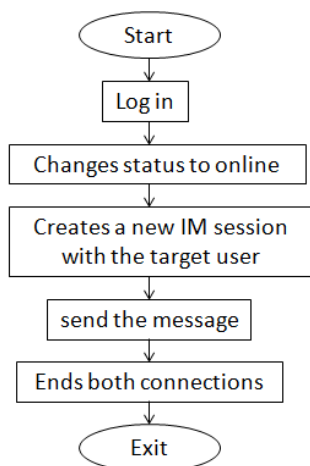


Figure 7. The flowchart of sendMsg

By putting the **sendMsg** tool on a web server, we can use a URL link to send messages to the user which has been pre-defined. For example,

- `http://hostname/sendMsg/index.html?message="test"`

The **sendMsg** consists of PHP scripts to create a new session with the target user. The configuration will include information about the sender and the recipient. By submitting the HTML form with the GET method, the variable *message* will contain the message that the sender wants to send to the recipient.

E. Get rid of special case

It may be annoying to get a lot of messages in one day. Therefore, it is necessary to send only important messages to administrators. For example, when one device is removed because of hardware failure, during the period of its maintenance, its status will certainly be DOWN. This should be regarded as a normal situation, instead of sending a warning to the administrator. The AED system provides a *White List* for administrators to define special cases to exclude. The white list will contain the IP address and port number of a device. An IP address refers to a layer-2 switch, so the AED system uses the (IP address, port) pair to specify a device connecting on the switch port. These special cases will be excluded from the log analysis, so it can prevent the AED system from sending false alarms.

F. Schematic diagram

The scenario of how an AED system works is shown in Figure 8. The administrator pre-defines an event at the command-line mode. The shell script will parse the log files and take some actions. Finally, the AED system will send a message to administrators.

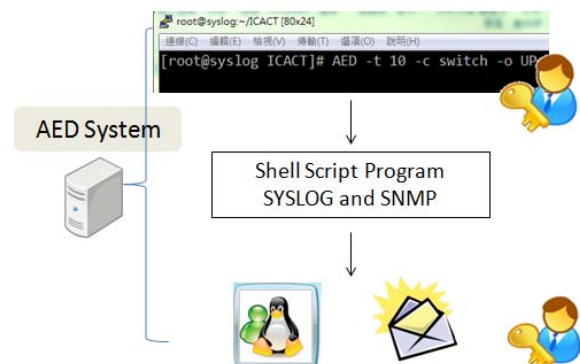


Figure 8. The AED system operation schematic diagram

IV. EXPERIMENTAL RESULTS AND ANALYSIS

After the real-time monitoring in Computer and Network Center of NCNU, the reports showed encouraging usefulness, while the two pre-defined cases in Section III successfully send out messages as expected.

Case 1 identifies the situation when there is a device plugged out from a layer-2 switch. The AED system will detect the event from the log which is stored by SYSLOG in every ten minutes. When the event happens, the AED will

collect all the data and send an MSN message to the administrator, as shown in Figure 9. The upper part of the picture with a penguin represents the AED system while the lower part of the picture with hats represents the manager. The message shows that:

- Port 1 on switch 10.77.1.240 has a device offline at 21:41:16 on 2011-10-10.
- Port 16 on switch 10.76.1.241 has a device offline at 21:45:11 on 2011-10-10.

Therefore the manager can see clearly which switches have something wrong.



Figure 9. The message from case 1

Case 2 intends to limit the bandwidth of an unexpected device. When the AED system detects the warning message which was issued when an unexpected device connecting to a switch, it will limit the bandwidth of the port to which the device connects, and send a message to the administrator, as show in Figure 10. The messages show below:

- Port 2 on switch 10.77.1.247 has a device online at 21:00:22 on 2011-09-11, and the bandwidth of the port is reduced to 128kbps.
- Port 8 on switch 10.75.1.247 has a device online at 21:01:00 on 2011-09-11, and the bandwidth of the port is reduced to 128kbps.

This means when the administrator gets this message, the problem has already been handled by AED, so that the administrator need not manually configure the switch.



Figure 10. The message from case 2

In addition to the MSN warning, the AED system also sends daily reports to the administrator as shown in Figure 11. With this report, the administrator can be fully aware of all accidents.

2011-10-13 AED system Report

```

root root@syslog.ncnu.edu.tw

===== 2011-10-13 AED system Report =====

== Case 1 - Total have 4 record
2011-10-13 13:44:33 The port 12 on switch 10.76.1.250 has a device offline.
2011-10-13 22:24:39 The port 24 on switch 10.75.1.244 has a device offline.
2011-10-13 23:29:08 The port 1 on switch 10.76.1.242 has a device offline.
2011-10-13 23:20:29 The port 8 on switch 10.77.1.249 has a device offline.

== Case 2 - Total have 3 record
2011-10-13 10:03:40 The port 5 on switch 10.78.1.244 has a device online,
and we limit the bandwidth of the port in 128kbps.
2011-10-13 13:44:45 The port 11 on switch 10.76.1.250 has a device online,
and we limit the bandwidth of the port in 128kbps.
2011-10-13 22:25:18 The port 13 on switch 10.76.1.247 has a device online,
and we limit the bandwidth of the port in 128kbps.

```

Figure 11. Daily report via Email

V. CONCLUSIONS AND FUTURE WORK

With the AED system, accidents can be solved in an effective and immediate way. Take NCNU for example, just as many other universities in Taiwan, it is necessary to limit each user's bandwidth in order to prevent the campus network from being abused by only a few users. This used to be controlled manually by daily update on each switch. If the manager is occupied by some other tasks, this configuration may be delayed. With the AED system, it can easily be done automatically. Through the pre-defined scenarios, managers need not worry about accidental breakdowns, and they can also be relieved from regular routine tasks.

Many network management systems include web management interfaces for easy configuration [12][7], and it will become our future work. Moreover, to complete the AED system, it should provide more pre-defined events which most administrators will need in managing their enterprise networks. Furthermore, right now managers have to pre-define each case in the AED system. If we can somehow create an intelligent system to learn from the managers by inspecting what instructions a manager takes when some situation happens, then this system can translate the instructions to scripts by itself. Such an automatic learning AED system will become much more powerful, which will be an interesting research topic for further exploration.

ACKNOWLEDGMENT

This work is partly supported by National Science Council in Taiwan under grants NSC 100-2218-E-029 -001.

We are grateful to the National Center for High-performance Computing for providing Taiwan Advanced Research and Education Network (TWAREN) as a perfect networking environment to support this experiment.

REFERENCES

- [1] Chia Yen, Yeu-Shiang Huang, "Two-Dimensional Warranty Model Considering Preventive Maintenance", National Cheng Kung University : Industrial and Information Management, Jun. 2005.
- [2] Demetres Antoniadis, "Michalis Polychronakis, Spiros Antonatos, Appmon: An Application for Accurate per Application Network Traffic Characterization", Proceedings of Broadband Europe, pp. 16. Geneva, Switzerland, 11-14, Dec. 2006.
- [3] Poul-Henning Kamp, Robert N. M. Watson, "Jails: Confining the omnipotent root", In Proc. 2nd Int. SANE Conf., Maastricht, The Netherlands, May 2000.
- [4] R. Gerhards , "The Syslog Protocol", IETF RFC 5424, Mar. 2009.
- [5] J. Case, M. Fedor, M. Schoffstall and J. Davin, "A Simple Network Management Protocol (SNMP)", IETF RFC 1157, May 1990.
- [6] P. Calyam, D. Krymskiy, M. Sridharan, P. Schopis, "Active and passive measurements on campus, regional and national network backbone paths", IEEE International Conference on Computer Communications and Networks (ICCCN), 2005.
- [7] Jiahai Yang, JianPing Wu., Yue You, "A Web-based, Event-driven Management Architecture", Fifth Asia-Pacific Conference on Communications and Fourth Optoelectronics and Communications Conference (APCC/OECC '99). Friendship Hotel, Beijing, China. Oct. 18-22, 1999.
- [8] Yen-Neng, Yang, "Implementation of SNMP trap notification framework", Master Thesis, Graduate Institute of Networking and Multimedia, National Taiwan University, Jun. 2010.
- [9] Wen HUANG, Dong-qing XIE, "The management and analysis model of network logs base on Syslog", Journal of Hunan University of Science and Engineering, May 2006.
- [10] Alfred V. Aho, Brian W. Kernighan and Peter J. Weinberger, "The AWK programming language", Addison-Wesley Longman Publishing Co., Inc., Boston, MA, 1987.
- [11] Leिताo Breno, Garcia Islene Calciolari, "sendmmsg: An Efficient System Call to Send Multiple Messages on Linux", 2011 Brazilian Symposium on Computing System Engineering (SBESC), Dec. 2011.
- [12] Kuo-Chiang Chiang, "Intelligent Network Management System", Master Thesis, Degree Program of ECE and CS Colleges, National Chiao Tung University, Sep. 2009.