Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 9 (2014) pp. 043-050

Monitoring Network and Service: A new Nagios services using smart notification management

Mohammad Ali Arsyad Mohd Shuhaimi[1], Zaheera Zainal Abidin[2], Syarulnaziah Anawar[3] and Zakiah binti Ayop[4]

[1234] Faculty of Information and Communication Technology
Universiti Teknikal Malaysia Melaka,
Hang Tuah Jaya, 76100 Durian Tunggal, Melaka.
musaz_ostrich@yahoo.com.my, zaheera@utem.edu.my, syarulnaziah@utem.edu.my and zakiah@utem.edu.my

Abstract: A new feature of services in Nagios has been added to the existing system which has no such services. The bandwidth monitoring and notification system are configured for alerting the network administrators when the bandwidth of the network in an organization hits a certain threshold settings. The system sent an email alert and sms notification to the network administrator for taking further action in order to maintain the Quality of Service (QoS) in the network. All the logs file of the Nagios actions is saved in the Nagios File Logs. The analysis was conducted from the case study and problem statements. Network Development Life Cycle (NDLC) was chosen as a methodology for implementing this system in the network. Nagios is installed inside Ubuntu 10 Operating System along with Multi-Router Traffic Grapher (MRTG) and Mail Postfix. MRTG and Mail Postfix were configured to be integrated with the Nagios System. On the client side, NSClient++ has been installed, for monitoring the bandwidth and performance of windows based on operating system. The Nagios services have been improved with the implementation of sms and emails notifications since the existing services have no such utilities. With the implementation of these services to Nagios, the performance could be even better for the future.

***Keywords*:** Nagios, MRTG, Network Monitoring, Email Notification, SMS Alert and Network Performance.

I. Introduction

Network monitoring describes the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator via email or notification in case of outages. It is a subset of the functions involved in network management. Network monitoring takes note of slowing or failing systems and notifies the network administrator of such occurrences. Such notifications can take the form of email messages, pager alerts, or plain old phone calls. No matter what form takes, network problem messages would be the highest priority. Network monitoring alert a network administrator to indicate the problems caused by overloaded systems, crashed servers, lost network connections, virus or malware infections and power outages, among other things. Network monitoring is commonly done by sending a ping or test to each computer or system on the network. If the system does not respond or takes too long to respond, the network monitoring system plays it roles. Pings are intended to be replied to instantaneously. In network monitoring, there are parameters which considered to measure such as bandwidth, latency, jitter and delay. These are common parameter in determining the performance of a network. Bandwidth is a measure of the amount of data passing through a network at a given time. For instance, a voice transmission by telephone requires a bandwidth of about 3000 cycles per second (3 KHz). A TV channel occupies a bandwidth of 6 million cycles per second (6MHz) in terrestrial system. In satellite based system a larger bandwidth of 17.5 to 72 MHz is used to spread the television signal in order to prevent interference. In computer networking, bandwidth in bit/s sometimes means the net bit rate, (also known as peak bit rate, information rate or physical layer useful bit rate), channel capacity, or the maximum throughput of a logical or physical communication path in a digital communication system. For example, bandwidth tests measure the maximum throughput of a computer network. The reason for this usage is that according to Hartley's law, the maximum data rate of a physical communication link is proportional to its bandwidth in hertz, which is sometimes called frequency bandwidth, spectral bandwidth, RF bandwidth, signal bandwidth or analog bandwidth.

FORMULA OF BANDWIDTH

$$bandwidth = \frac{\sum bits}{s} \qquad (1)$$

The network monitoring process is incomplete without the assistance of monitoring tools. In fact, hundreds of free tools provided to assist network engineer or administrator to govern the network, such as PRTG and MRTG. One of the powerful network monitoring is Nagios. Nagios is a free, open-source web-based network monitor developed by Ethan Galstad. Nagios is designed to run on Linux, but can be also be used on UNIX variants. Nagios monitors the status of host systems and network services and notifies the user of problems. In common with many open source utilities, installation requires a degree

of system administrator experience. Nagios is a primary tool used to diagnose, prevent, and deal with network problems. The increasing of high bandwidth and mission critical application over Local Area Network (LAN) into Wide Area Network (WAN), demands more effective monitoring tools. Without a proper tools that can analyze and display network traffic and any related problem, a network admin is limited to the time-consuming try and error method to try identifying a problem. Nagios is definitely not for the novice. However with a wide range of features, including a number of web interfaces, Nagios is a very useful, feature rich monitoring tool. A large number of plug-ins available from the Nagios Library, meaning it could be customized according to requirements. Amongst others, Nagios monitors services such as SMTP, POP3, HTTP, PING and resources such as disk and memory usage, log files, processor load that integrates with the Sensatronics IT Temperature Monitor to allow monitoring and alerting of server room and device temperature at certain parameters. Nagios allows scheduling if there is network outage which the host can be suppressed and provides service notifications. Nagios gives users the flexibility to develop custom host and service checks. All the plug-ins is available for download from the Nagios library. It is possible to set up a hierarchy of alerts for instance if alerts are not responded to. The monitoring daemon runs intermittent checks on hosts and by using external plugins which return status information to Nagios. Current status information, historical logs, and reports can all be accessed via a web browser. Nagios runs on Linux and UNIX variants.

II. Related Works

The traffic on the network is generated by hundreds of devices and applications. Without the proper tools that can interpret, analyses and display network traffic and any related problem, a network admin can save time and energy to identify the network problem. With Nagios application, plug-ins and configuration such problem can immediately been detected. The bandwidth alert system monitored the maximum line bandwidth which transferred the current activities; therefore, it sent an alert to the network admin if the bandwidth usage hits a certain threshold, without interfering with interactive user or other network applications. Bandwidth Alert System provide better bandwidth performance by sending a warning, if the bandwidth usage arising, an emergency alert will be send to network admin for further actions. This is a step of early prevention of bandwidth outage in a network. To keep a network performing on the top-notch condition, the application as below will be developed:

- Nagios integrated with Multi-Router Traffic Grapher (MRTG)
- Nagios with Notifier via email
- Nagios with Restart Remote Server
- Developed and tested in Wireless Network

Network Monitoring Tool eases the work of every network administrator. Nagios is a real time network tool used to analyze interpret and display network traffic. The workstation and client can monitor some the traffic flow in the network without disturbing the network at the same time. It also provides tools for technical control and performance of the system. The whole system can be viewed as combined structure with important process. Nagios application also presents the network bandwidth usage and also can notify the network admin via email if the network down or the bandwidth hits a certain threshold. Integrated MRTG also enable the network admin to view the bandwidth congestion during the peak hours. We propose the new services in Nagios which capable of monitoring network, bandwidth, alert via email and generate graph. Network monitoring is a part of the network. Real-time network analysis helps detect network faults and performance quickly thus preventing the network to down.

A. Nagios integrated with Multi-Router Traffic

- **Grapher (MRTG)**
  - Ability to monitor bandwidth traffic
  - Ability to determine the lowers and maximum bandwidth
  - Ability to generate graph

B. Nagios with Notify via email

- Ability to alert the network admin via email whenever there is a problem in the network and the bandwidth usage has hit a certain threshold.

C. Nagios with restart remote server

- Ability to restart the server from remote site.

III. Literature Review

Limoncelli et. al present a comprehensive look at best practices in managing systems and networks in their book, Practice and Network Administration[1]. The authors indicate the importance of monitoring to avoid a system from being down in a period of time before action can be taken by the administrators. There are two types of monitoring; historical monitoring and real-time monitoring. The former provides long-term data on uptime, use and performance while the latter provides information on current state of service [2].

Wikipedia lists sixty-six different products of free network monitoring software; some of them are open source projects under a General Public License. This paper will discuss on real-time monitoring with focus on notification of problem.

A. Monitoring Network Quality of Service in a Dynamic Real-Time System

Network monitoring is an important part of network resource management. The vast growth of the computer network and internet make a network monitoring more complicated and more challenging. Netmon is designed [3], for performance monitoring of a packet data network, which measure network performance statistic using SNMP information polled from backbone router. However, this approach does not provide information of computer host and network path [4]. Hence, it is not suitable to be used as network monitoring tool for the resource management middleware. Another network monitoring tool that had been considered and actually tested in the course of this research was REMOS (Resource Monitoring System), which is currently being developed at Carnegie Melon University [5]. REMOS allow network-aware application to obtain both static and dynamic information

about network. The network uses SNMP and benchmark techniques to collect status information.

B. SoftPerfect Bandwidth Manager for Windows

SoftPerfect bandwidth Manager is a full-featured traffic management tool for Windows that offer cost-effective bandwidth control and quality of service based on built-in prioritized rules. These rules can specify a bandwidth shaper, bandwidth limit for each Internet user. This kind of software often called bandwidth shaper, bandwidth limiter or traffic shaper. With SoftPerfect Bandwidth Manager, you can apply speed-throttling rules to specified IP addresses, port and even network interface with no change to existing network infrastructure. This rich feature is easily managed via the intuitive Windows GUI.

C. Hierarchical Filtering-based Monitoring System for Large-scale Distributed Application

Monitoring is an essential process to observe and improve the reliability and the performance of large-scale distributed (LSD) application. The monitoring system is dynamic since the monitoring demand can be added, delete and modified at runtime with no interface with the running application [8]. These design features distinguish the monitoring architecture with the other open source monitoring system. A survey and evaluation of the related work in even filtering and monitoring are done in respectively [9]. The nagios services have been added with new feature of services implemented by [10] in improving the network performance. The new services are such as Email notification, sms alert, flexible alert, reporting and remote reboot server. In [11] has performed the evaluation criteria in comparing services provided between the existing nagios and nagios with the new feature of services.

IV. Analysis

Requirement analysis is fundamental to the network design which is about to understanding the design environment. This part is consists of identifying, gathering and understanding the system requirement and their characteristic and developing thresholds for performance to get the better accuracy for the network.

The challenge in this phase is to gather the requirement to determine the system and network services that the network will support. The increasing usage of application through the network can harm the network performance. Bandwidth outages is one of the main problem arise when many people connecting to the network and sharing the resources to the whole network.

During analysis phase, Multi-Router Traffic Grapher (MRTG) is used to collect data inside the router and later, Nagios will be integrated with MRTG so that Nagios can monitor and notify the network admin if the bandwidth hits a certain threshold.

MRTG consists of a Perl script which uses SNMP to read the traffic counters of your routers and a fast C program which logs the traffic data and creates beautiful graphs representing the traffic on the monitored network connection. These graphs are embedded into web pages which can be viewed from any modern Web-browser.

In addition to a detailed daily view, MRTG also creates visual representations of the traffic seen during the last seven days, the last five weeks and the last twelve months. This is possible because MRTG keeps a log of all the data it has pulled from the router. This log is automatically consolidated so that it does not grow over time, but still contains all the relevant data for all the traffic seen over the last two years. This is all performed in an efficient manner. Therefore you can monitor 200 or more network links from any halfway decent UNIX box.

MRTG is not limited to monitoring traffic, though. It is possible to monitor any SNMP variable you choose. You can even use an external program to gather the data which should be monitored via MRTG. People are using MRTG, to monitor things such as System Load, Login Sessions, Modem availability and more. MRTG even allows you to accumulate two or more data sources into a single graph.

In network research, possible scenario is a technique where a program simulates the characteristic of a network. From the use of scenario, it can be performs by this simulation either by calculating the interaction between the different network device such as host, routers, data links and packets using mathematical formulas, or actually capturing and playing back network parameters from a production network. Using this input, the behaviour of the network and the various applications and services it supports can be observed in Nagios.

This project will be adding some function to Network monitoring Tool Nagios with the function of monitoring bandwidth and notify the network admin via email if current network bandwidth traffic hits a certain threshold specify by the network admin. The bandwidth data collected by MRTG is shown in Figure 1.

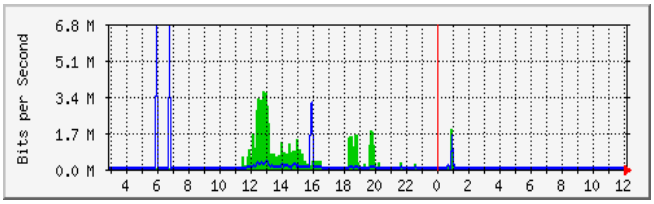

Figure 1: Bandwidth data collected by MRTG

We construct two possible scenarios for future experiment based on bandwidth congestion during peak hour and off-peak hour.

Scenario 1: Bandwidth Congestion during Peak Hour

A peak hour is a part of the day during which traffic bandwidth congestion on network of an organization is at its highest. Normally, this happens twice a day. Once in the morning and once in the evening, the times during when the most people using the internet to surfing and doing work.

During the peak hour, the speed of the internet and intranet will be greatly dropped. User will experience slow speed of browsing internet, the webpage load is too slow and the worst case scenario is the network might be down for some time which eventually will cost them a great fortune.

Multi-Router Traffic Grapher (MRTG) which is installed in the server will get the bandwidth traffic from the wireless router every five minutes interval. MRTG then will generate a graph from the traffic collected from the wireless router. After the graph is generated, Nagios will read the graph and from the graph reading, Nagios will calculate the maximum incoming and outgoing bandwidth, the minimum incoming and outgoing bandwidth and the average bandwidth. From the reading, if Nagios detects bandwidth usage has hit a certain threshold; it will notify the network administrator via email. An example of MRTG graph is generate during peak hour is shown in Figure 2.

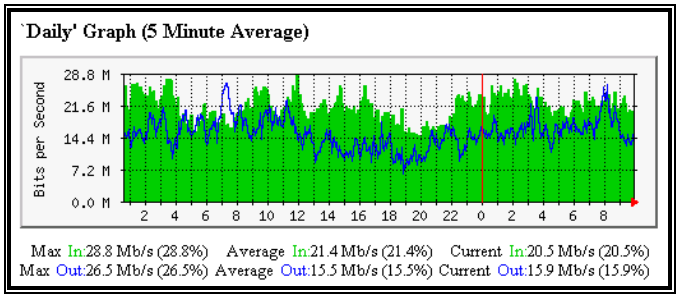

Figure 2: Example of MRTG during Peak Hour

Scenario 2: Bandwidth Usage during Off Peak

Off peak-time is usually refers for the time few worker do their work or task. From that, the usage of the network is not higher than the peak time because the number of user usage is lower. This is usually happens at early morning day where almost people is prepare to start their work. The other time this situation happen is at afternoon during break-hour where almost people take time to break and take a lunch. At this time the network traffic usually smoother and it use lower traffic than peak hour.

Multi-Router Traffic Grapher (MRTG) which is installed in the server will get the bandwidth traffic from the wireless router every five minutes interval. MRTG then will generate a graph from the traffic collected from the wireless router. After the graph is generated, Nagios will read the graph and from the graph reading, Nagios will calculate the maximum incoming and outgoing bandwidth, the minimum incoming and outgoing bandwidth and the average bandwidth. From the reading, if Nagios detects bandwidth usage has hit a certain threshold; it will notify the network administrator via email.

V. Experiment Setup

The experiment is done as in Figure 3, setup in wireless local area network with 300 Mbps speed. The Nagios server is installed at the server computer. In the Nagios server, there are some services installed in that particular server which are Web Server (Apache), Mail Postfix and Network Monitoring Tool (Nagios). The server was monitoring the windows client and the wireless router since Nagios is capable of monitoring network, hard drive space, uptime and down time of a node.

The client side is installed with NSClient++ which act as Nagios service for the client side and send data to the Nagios Server. From there, Nagios was able to determine the size of the network and where the nodes are located. An alert is sent to the network admin if there a problem with a host and most importantly when the bandwidth hits a certain threshold set up by the network admin. The tests are done to ensure the data collected are satisfied to the parameter, have been selected. All of the services are configured in order to test the Network Monitoring Bandwidth Alert System. Multi-Router Traffic Grapher is used to generate the bandwidth usage by visualize the bandwidth usage for each 5 minutes in the form of graph.

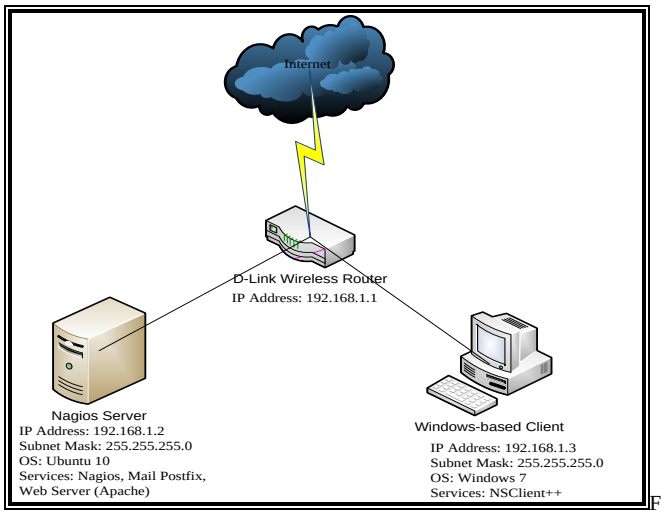

Figure 3: The logical design of the proposed model

Thus, a threshold is set and Nagios Server shared resources to the client. While the client downloading the sharing resources, Nagios monitored the bandwidth usage inside the wireless router. When the bandwidth usage almost reaches a certain threshold define by network admin, a warning alert is sent to the network admin via email. If the bandwidth usage constantly arising, the critical alert would be send to the network administrator via email. The alert is stored as a log inside the Nagios configuration. If the email was unable to send to the network admin, the log files is generated and informing email cannot be send.

Figure 4 and 5 show the architecture of Nagios with and without the Email and SMS notification. It explains which part of configuration done in Figure 3 clearly visualized in layer affected in Figure 5.

A. Test Environment

The Nagios is tested on wireless network environment with the support of Wide Area Network (WAN) for the ability to send notification to email and GSM Modem for the ability to send Short Message Service (SMS) to the network administrator as in Figure 6. A shared folder is created for sharing so that the client can download the files in the shared folder for Nagios to examine the bandwidth usage of the client.

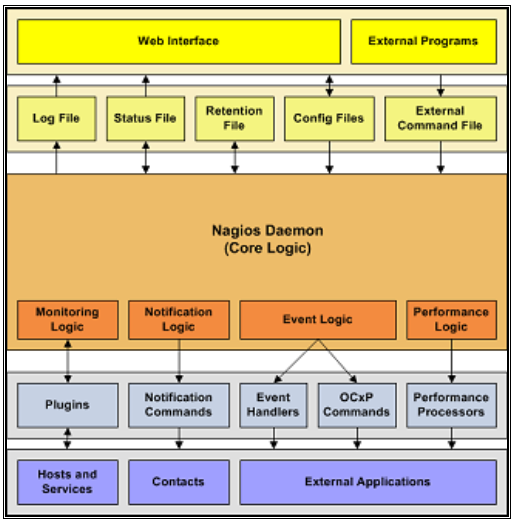

Figure 4: Nagios Architecture
(before implementation of SMS and email notification)

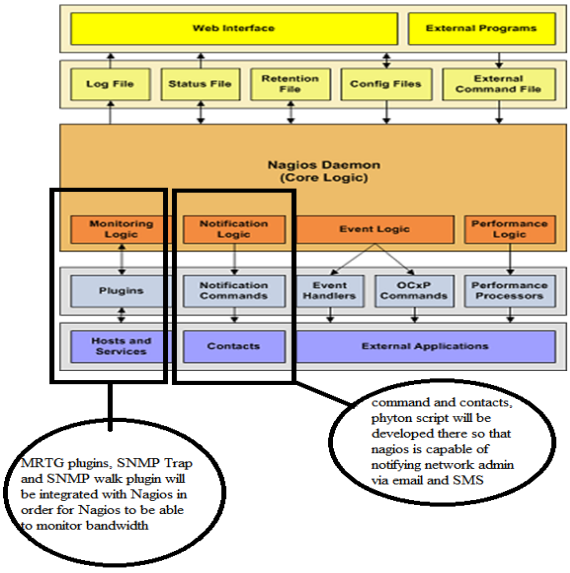

Figure 5: New Nagios Architecture
(after the implementation of SMS and email notification)

The testing process consists of processes involve changing of configuration at Nagios.cfg, Contact.cfg and Commands.cfg of Nagios. Each change occurred in different test phase in order to ensure its effectiveness.

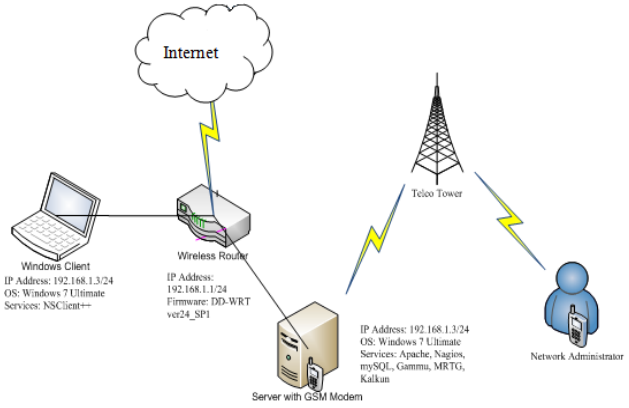

Figure 6: SMS and Email Notification Connectivity Environment Setup

Service monitoring can consist of a variety of tests. Feher and Sondag has outlined three forms of test to verify the connection between a host and server and whether they are successfully connected to the network. First, using ping test to monitor the availability of access points and monitoring connectivity to remote locations. A better alternative is to test the establishment of a connection on a port. The third method would be evaluating a service response, for instance by checking status coded replied by a Web server. The second method is demonstrated in [14] and the third method is demonstrated in [1].

In this project, we are using the ping test for its simplicity and to avoid overhead introduce by other methods. The network administrator tested the connectivity by 'ping'ing from the server to the client. After tested the connectivity, the network administrator need to test the availability of the sms and email notifications services that is newly added into Nagios.

B. Test Result

The test result can be seen in Nagios Log Result as shown in Figure 8.

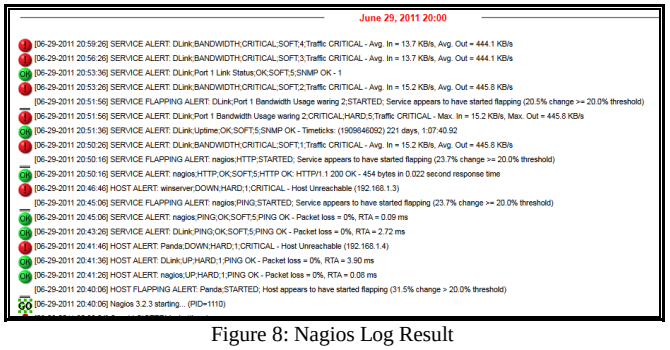

Figure 8: Nagios Log Result

If the client bandwidth usage hits the threshold, Nagios automatically send the notification to the network administrator via email and SMS, as in Figure 9 and 10.

Figure 9: Email Notification from Nagios

SMSCNumber	varchar(20)		+60120000015
Class	int(11)		-1
TextDecoded	text		-***** Nagios ***** Notification Type: PROBLEM Service: BANDWIDTH Host: DLink SWITCH Address: 192.168.1.1 State: CRITICAL Date/Time: Wed Jun 29 15:53:23 MYT 2011 Additional Info: Traffic CRITICAL - Avg. In = 13.6 KB/s, Avg. Out = 440.3 KB/s
ID	int(10) unsigned		18
SenderID	varchar(255)		
SequencePosition	int(11)		1
Status	enum	--	SendingOKNoReport

Figure 10: SMS Alerts stored in MySQL

Figure 11 shows the Nagios alert messages at the host. The node is identified as green in colour to show that the device is enabled or 'ON' mode. However, if it is in red it means the node is down or 'OFF' mode.

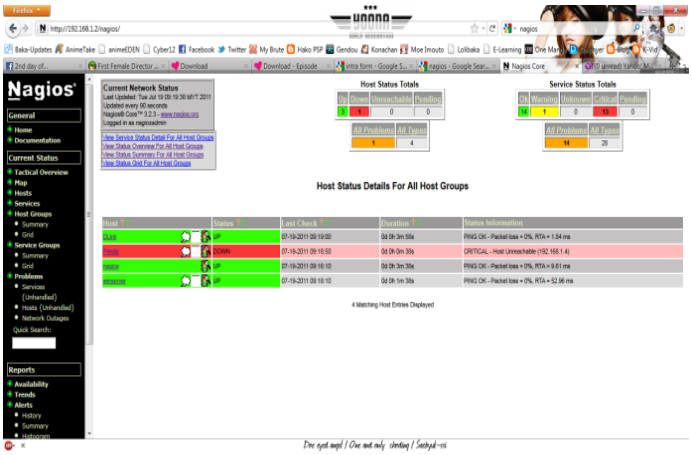

Figure 11: Nagios (Host Based)

Figure 12 shows the details of services with the notification information in web-based form. This information is very important for network engineer to fully optimizing the bandwidth utilization in the network performance.

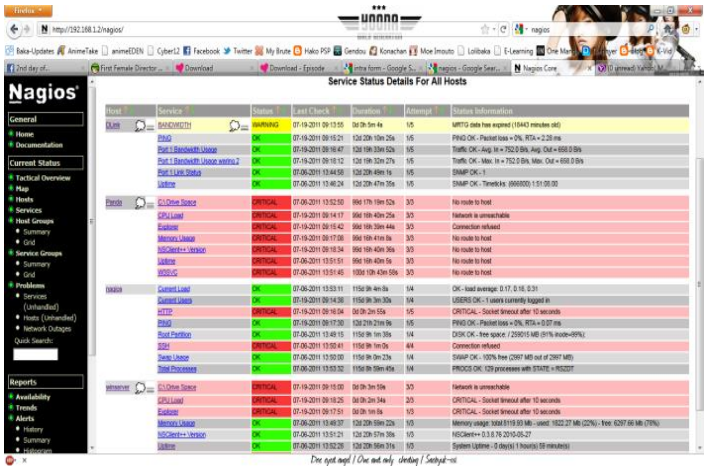

Figure 12: Nagios (Services Details)

Figure 13 shows the web-based notifications of email and SMS of the new services implemented in Nagios.

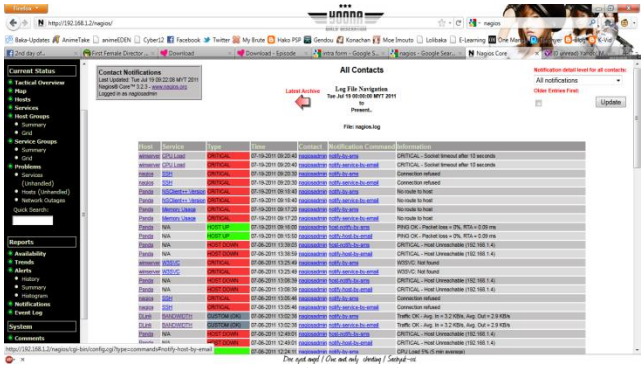

Figure 13: Nagios (Notifications of Email and SMS)

Figure 14 shows the network bandwidth utility represented in graph. It means the new service of nagios has been implemented.

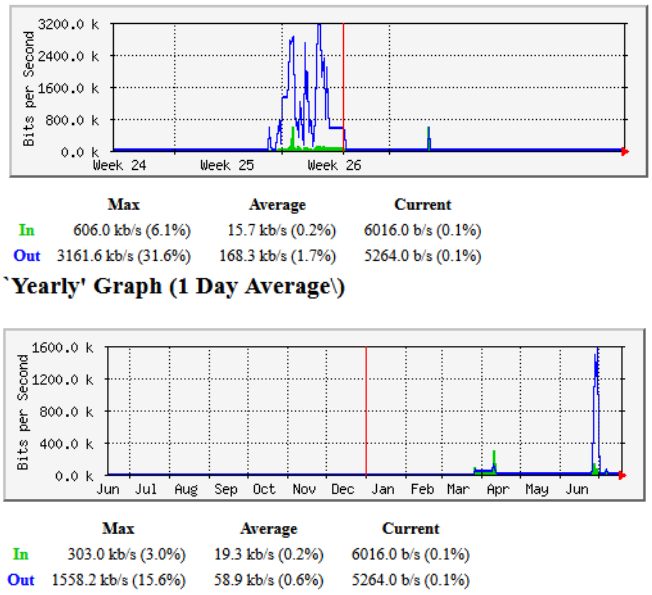

Figure 14: Nagios (Graph of Network Performance)

VI. Evaluation

This part intends to evaluate the enhanced Nagios service with the existing. The evaluation itself is interesting in how to differentiate both systems based on the usability of the system to complement the criteria as outlined in [11]. The criterions are configuration data store, scalability, reporting and application interfaces.

For more understanding on evaluation and comparison of how well each system performs network monitoring functionalities, we represent the evaluation of both systems in Table 1 under the following criteria:

- Configuration Data Store
- Scalability
- Reporting Capabilities
- Application Interfaces
- Restart Remote Service
- Error Message

	Existing Nagios	Nagios + New Features
Configuration Data Store	Simple format of flat files. Allow changes and addition of new service checks using various scripting languages.	Simple format of flat files. Allow changes and addition of new service checks using various scripting languages. GUI web based flat files format stored in MySQL.
Scalability	Ability to run multiple monitoring servers and forward results to a central server for checking the results.	Ability to run multiple monitoring servers and forward results to a central server for checking the results.
Reporting Capabilities	Keeps alert history alerts and downtimes of all hosts and service checks by default. Various reports of availability can be created for individual servers, host groups and specific checks. Allow administrators to store comments with time stamps in storing the work history and log of notes for the required hosts.	GUI web based 1- Keeps history log and service details at the server site. GUI web based 2- Email Notification and sms alert.
Application Interfaces	GUI web based. Hosts and server can be fully controlled using command line using text editor or external tool.	GUI web based interface of graph creation and log files. Hosts and server can be fully controlled using command line using text editor or external tool.
Restart Remote Service	One of the Event Handler components which allow hosts to function from remote area.	Allow the server to be restarted remotely if the computer hang and not function to according.
Error Message	No error message	Perform error message when the email and sms are not notified by the administrator.

Table 1: Existing versus New Featured Nagios Evaluation

The evaluation is said [11] based on four criteria such as configuration data store, scalability, reporting and application interfaces. [10] stated that Nagios is a popular open source monitoring tool which collect samples of performance indexes (CPU utilization, memory utilization, disk utilization and network throughput) at the system and the application level.

VII. Discussions

Nagios has been one of the free monitoring tools which able to customized according to demands. However, the limitation of Nagios is when the internet is down and Nagios would not be able to send an email to the network administrator. This is because Nagios notification is completely relying on internet based connection to alert the network administrator. Due to this issue, email notification and sms alert services are implemented with the nagios.

During the observation, some strengths of the Nagios system have been highlighted. One of the strength of the nagios alert and notification is the alert is send in real time environment. For example, if the bandwidth usage has passed it threshold at 5.00 p.m. then the Nagios alert will notify the network administrator at 5.05 p.m. Why the alert late five minutes? It is due to the Nagios services that monitor the bandwidth in five minutes intervals. Also, Nagios has early stages of warning. Nagios first will send a warning alert to warn the network administrator that the bandwidth usage almost hits the specified threshold. And if the bandwidth usage hits the threshold, the critical alert will send instead.

Original version of Nagios can't monitor bandwidth in the network environment. Since the Nagios has been configured to integrate with Multi-Router Traffic Grapher (MRTG), Nagios has the ability to monitor bandwidth of a network and generate graph of bandwidth usage. The graph is updated in five minutes interval.

VIII. Future Work

Nagios can be configured to be integrated with GSM Modem so Nagios can both send alerts to network administrator email and hand phone. Nowadays, people need hand phone in their life. Therefore, it is hard to see people separated with his or her hand phone.

The second recommendation is to be able to configure the Nagios and adding some coding to make Nagios be able to not only monitor bandwidth usage, but also to control bandwidth in the network. Thus, if the bandwidth in the network is unusually high, network administrator can control the bandwidth by using Nagios. This makes Nagios a very powerful Network Monitoring Tool since Nagios will be able to monitor the network and at the same time Nagios also can control the bandwidth congestion in the network.

It is a convenience to the network administrator however another issue which needs to think about is security. Nowadays, people hacked into email server and other systems with intension to harm the data and system. Therefore, what will be the mechanism to protect the alert or email sending from the server to the administrator? How to prevent the

hacking activities in securing the channel of data communication?

IX. Conclusions

The implementation of the Nagios email notification and sms alert have increased the reliability of the existing Nagios settings. The notification and alert help improved the Quality of Service (QoS) of the network and preventing the network outages. Network outages produce loss to organization. It was sensitive to bandwidth, latency and throughput of the network. The server or hosts can be easily restarted remotely and the access control management is done in real time. Therefore, with the implementation of new services in Nagios gave a value added to the services in improving the network performance in an organization. In other hand, Nagios is not only free source tool but also can be customized according to the needs of users in an organization.

References

[1] Limoncelli, Thomas A. ; Hogan, Christina J. ; Chalup, Strata R.: Practice Of System And Network Administration, The (2nd Edition). 2 : Addison-Wesley Professional, 2007

[2] Silver, T.M., Monitoring network and service availability with open-source software (8-22), Information Technology and Libraries (ITAL) volume 29, number 1, march 2010.

[3] Alexey Rogozhkin, "Deploying Nagios Monitoring Services on Secured Red Hat Enterprise Linux 3", Global Information Assurance Certification Paper, SANS Int., 2005.

[4] Online Resources: "*Bandwidth Monitoring with Nagios and MRTG*", NetworkGod"s Blog, 2009, Retrieved on April 2011 from http://www.networkgod.net/archives/121

[5] Online Resources: "*OpenBSD Installation Guide",* OpenBSD, 2010, Retrieved on April 2011 from http://www.openbsd.org/faq/faq4.html

[6] Online Resources: "*Nagios Documentation",* Nagios, 2010, Retrieved on April 2011 from http://www.nagios.org/documentation

[7] Online Resources: "*Nagios Plugins",* Nagios, 2010, Retrieved on April 2011 from http://www.nagiosexchange.org

[8] Ehab Al-shaer and Hussein Abdel-wahab and Kurt Maly, "Hierarchical Filtering-based Monitoring System for Large-scale Distributed Application", 10th International Conference on Parallel and Distributed Computing Systems, 1997.

[9] Hong Chen, "Monitoring Network Quality of Service in a Dynamic Real-Time System", Fritz J. and Dolores H. Russ College of Engineering and Technology of Ohio University", 2003.

[10] Bin Mohd Shuhaimi, M.A.A.; Binti Roslan, I.; Binti Zainal Abidin, Z.; binti Anawar, S., "The new services in Nagios: Network Bandwidth Utility, Email Notification and SMS Alert in Improving the Network Performance", in *IEEE*, International Conference on Information Assurance and Security (IAS), 2011, pp. 86 – 91.

[11] Online Resources: "SCF/FEF Evaluation of Nagios and Zabbix Monitoring Systems", 2009, Retrieved on Mac 2012 from http://cd-docdb.fnal.gov/cgi-bin/RetrieveFile?docid=3277;filename=nagios_zabbix_evaluation.pdf;version=1.

[12] Mauro Andreolini, Michele Colajanni and Riccardo Lancellotti, "Assessing the overhead and scalability of system monitors for large data centers", ACM, 2011.

[13] Joshua Etkin And John A. Zinky, "Development Life Cycle Of Computer Networks: The Executable Model Approach", IEEE Transactions On Software Engineering, No. 9, September 1989.

[14] Feher, J., & Sondag, T. (2008). Administering an Open-Source Wireless Network. Information Technology Libraries, 27(3), 44-54.

Author Biographies

Mohammad Ali Arsyad bin Mohd Shuhaimi graduated in 2006 from MARA Junior Science College Muadzam Shah, Pahang. Then, he graduated in 2007 from Perak Matriculation College. He entered University of Technical Malaysia, Malacca (UTeM) in 2008 until 2011 and will receive his Bachelor of Computer Science in Computer Networking in October 2012. His research interests include network monitoring, network security and remote monitoring system.

Zaheera Zainal Abidin received Bachelor of Information Technology from University of Canberra, Australia, 2002. She joined ExxonMobil Kuala Lumpur Regional Center as a Project Analyst while waiting for graduation. She completed her MSc. in Quantitative Sciences (2004) and MSc. in Computer Networking (2008) from Universiti Teknologi MARA, Shah Alam, Selangor. She served as a lecturer at Universiti Kuala Lumpur (2005-2009) and Universiti Teknikal Malaysia Melaka (2009 – present). Her research interests include biometric security, steganography and image processing.

Syarulnaziah binti Anawar received Bachelor of Information Technology from Universiti Utara Malaysia, 2001. She joined University of Technical Malaysia, Malacca (UTeM) as a Tutor in Faculty of Information Technology (2001). She completed her MSc. in Distributed Computing (2003) from Universiti Putra Malaysia. She returned back to UTeM as a lecturer. Her research interests are pervasive system, network optimization and autonomous computing.

Zakiah binti Ayop received Bachelor of Computer Science from University of Technology, Malaysia, 2000. She joined University of Technical Malaysia, Malacca (UTeM) as a Tutor in Faculty of Information Technology (2001). She completed her MSc. in Distributed Computing (2003) from Univeristy of Putra, Malaysia. She returned back to UTeM as a lecturer. Her research interests are trust and reputation system, information and network security; and crowdsourcing.