Development of Email and SMS Based Notification System to Detect Abnormal Network Conditions: A Case Study of Faculty of Business Administration, Rajamangala University of Technology Phra Nakhon, Thailand

Kreadtisak Lappanitchayakul
Division of Information System, Faculty of Business Administration
Rajamangala University of Technology Phra Nakhon
Bangkok, Thailand
kreadtisak.l@rmutp.ac.th

***Abstract*— The developed network monitoring system detected and alerted the abnormality of appliances in the network of Rajamangala University of Technology Phra Nakhon by applying ICMP Protocol (Ping). Moreover, the developed system displayed the connection status of network appliance and record of appliance connection on a website so it was easy to monitor and caution the possible problems. When the network monitoring system detected the abnormality in the network connection, it sent E-mail and SMS alert to the system administrator to make him aware of the location of abnormal appliance and fix the problem. Further, the developed system facilitated the system administrator to check the connection record of the appliance in the system to set the preventive plan.**

Keywords—Network Monitoring System; SMS Alert System; Email Based Notification System

I. INTRODUCTION

Information technology is a key factor in the change of Thailand to enter Thailand 4.0 and Association of South East Asian Nations (ASEAN) [1]. For this reason, government and private agencies adjust themselves in various aspects, including develop information technology to be consistent with the current mission of each agency.

Rajamangala University of Technology Phra Nakhon is awakened and respond to the government policy to become the educational hub of ASEAN [2]. Many factors are required in order to become the educational hub such as instructional planning, information technology, personnel, and other concerning elements. Although Rajamangala University of Technology Phra Nakhon is well-prepared with all components, there are some problem with information technology system. As Rajamangala University of Technology Phra Nakhon that consisting of four campuses (Thewes Campus, Chotiwet Campus, Bangkok Commercial Campus, and North Bangkok Campus), the network system is implemented to exchange internal and external information. The central unit (Thewes Campus) is in charge of the entire network system. When a problem occurs with some devices, users such as lecturers and University staffs will inform the Information Technology staffs at each center. Then the staffs will report to the main system administrators through telephone so they can fix the problem at the reported center. However, staffs from the main center will roughly locate the device with a problem, they will only know if the malfunction occurred at any of the centers through the person who notifies, but will not know the exact type and location of the malfunctioning device, due to informers and IT staffs cannot identify such information. As such, administrators must monitor all devices in that center, to determine which device is broken. Since each center has a large number of devices such as Host computer, Access Point, and more than 100 Switches, it is difficult to check every single device and it also wastes a lot of time. Moreover, the university is experiencing a problem with insufficient staffs from the main center and it results in a long period of inspection. This affects the operation of the organization in terms of communication within their own network and the outside organization which have to stop for a long period of time. For this reason, the university has solved the problem by increasing the number of staffs but it still does not reach demand. The prior solution to the problem is not the correct answer, not only wasting budget on hiring staffs but also wasting time and it is not the effective Human Resource Management.

Therefore, the software that currently available in both License and Freeware were brought to solve the problem. The software will detect the malfunction in the network of each center through the computer screen instead of through telephone. Whenever the system cannot connect to the device, the system will notify to the administrator's email by identifying the IP address and the name of the malfunctioning device so the administrator can acknowledge the problem immediately. However, the notification software has not

978-1-5386-7516-8/18/$31.00 ©2018 IEEE

identified the type and location of the malfunctioning device. Moreover, the notification email also has the limitation in internet network that if the network originating from the source and/or destination is not available, the staffs at the main center will not receive the notification email. As such, the developed system in this research added one more notification which is via SMS. It also records the connection history of all devices in the network which is useful for administrators to diagnose problems that may arise in the future.

The researcher developed the Network Monitoring system to be used in Rajamangala University of Technology Phra Nakhon. The system will notify the problem through email and SMS, it also will identify the type and location of the malfunctioning device accurately and effectively. This developed system will reduce the staffs' working time as well as the number of staffs because the staffs can acknowledge the type and location of the malfunctioning device correctly and in time.

II. RELATED WORKS

Network Monitoring [3-4] Software performs a function to monitor the status of network system where device is connecting to computer software. Switch may be involved in monitoring software. There is various software available in the market as follows.

A. *WhatsUp Gold*

WhatsUp Gold [5-7] is the monitoring program for network and services system in server as shown in Figure 1. The alert will signal or the text will be sent from the program to notify the location of the problem via email to a system administrator for the instant solution which help to minimize the damage to the system. Its performances are as follows.

- Search for Ping or Scan port or services running on Windows, or Unix/Linux from IP Address by working with SNMP Protocol.
- Have alert notification via e-mail, sound, or sms (sending via sms requires SMS gateway or sms gateway through internet).
- Display graph and diagram of all different colored devices.
- Set the alert form to notify the system administrator of the change of device or device parts value.
- Report the change of device or device parts to the system administrator.
- Set the alert for threshold monitoring as desired to be compatible with device function.
- Check report on Tablet or smart phone

B. *PRTG Network Monitoring*

PRTG Network Monitoring [8-9] is a program to detect the application of device in the network supporting SNMP, WMI, and other relating to monitoring as shown in Figure 2. Then, it creates graph to the user to analyze the application and develop the efficiency and effectiveness of operation. Its performances are as follows.

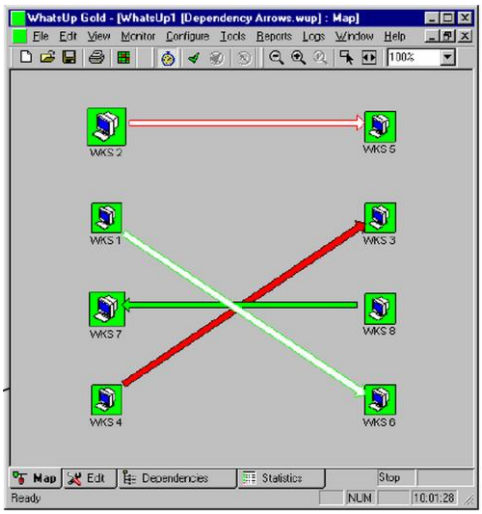

Fig.1. WhatsUp Gold [7]

- The program can search for the networking devices by scanning.
- The program display result in graph and report format.
- The program can notifies the abnormal function via e-mail
- The program monitors the status of LANs, WANs, servers, websites, appliances, URLs, and others.

C. *The Dude Network Monitoring*

The Dude Network Monitoring [10-11] is a freeware program that monitors the network whether there is a damage of the network or not as shown in Figure 3. The program comprises of two main parts Network MAPs and Chart with the following performances.

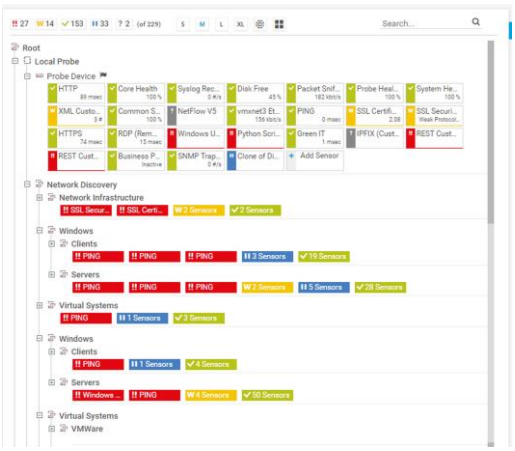

Fig. 2. PRTG Network Monitoring [9]

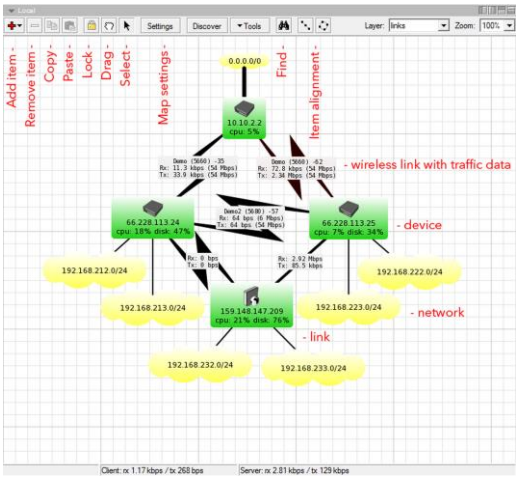

Fig. 3. The Dude Network Monitoring [10]

- Display the damage device or service.
- Scan system searches for networking device, no extra device required.
- Monitor both devices and Link if it is functioning and notify with the alert.
- Check service such as HTTP, SMTP, SNMP from the device.
- NETWORK MAPs.
- Display details of each equipment and device.
- Support SNMP V1 and V2.

D. ZENOSS

ZENOSS [12-13] monitors and searches the networking devices by scanning all devices in subnets and draws the figure or diagram as shown in Figure 4. There are two versions: Zenoss Core and Zenoss Enterprise with the following performances.

- Examine and monitor via Web Browser.
- Searches for networking device by scanning.
- Display networking chart.
- Notify problem via e-mail.

III. THEORIES

A. ICMP

ICMP [14-16] is the report from the system to identify what is happening to the data transfer. The common problem found is unable to transfer or the receiver cannot receive data. ICMP protocol is used to exchange the data between the server and networking devices. ICMP protocol is functioning with IP protocol in the same system. Therefore, ICMP protocol is a tool for testing network. For example, Ping is used to test whether the server is operating normally. Then, it accesses

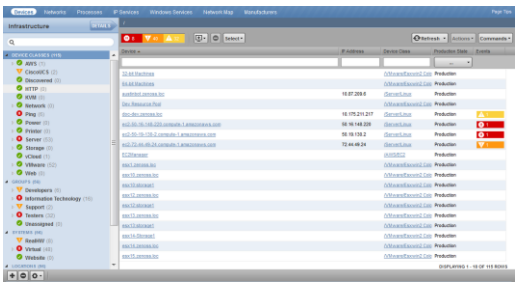

Fig. 4. ZENOSS [12]

ICMP protocol and send message back from the terminal.

B. Ping Flood

Ping Flood [17-19] is an attack method used in former DoS that transfers large packages to the terminal. Principle of Ping Flood is to send ICMP Echo Request package, which is the same package from Ping command, to the target rapidly. The device has to reply ICMP Echo Reply continually and the target may stop operating.

IV. DESIGN OF NETWORK MONITORING SYSTEM

The design of Network Monitoring system implements ICMP Protocol to monitor the function of networking appliances. The researcher recognized the possible problems with the system regarding Ping flood which security system of organization will be considered the network attack. The data transfer package is limited at 32 bytes. The researcher designed the Network Monitoring as shown in Figure 5.

In this case, the researcher has designed a system that supports devices such as Access Point and Switch Layer 3. In this research, the researcher simulates the test with the host computer, both internal and outside of the university as follow;

- A host computer for university website.
- A host computer for e-Calendar service.
- A host computer for Learning Management System
- A host computer for Budget Planning & Management
- A host computer for Human Resource Management
- A host computer for reporting IT problems.
- A host computer for enrollment services.

The developed system has the following features and functions:

1) Network Monitoring Appliance monitors the function of appliances networking via LAN by Ping to IP Address via ICMP Protocol. The appliance's performances are as follows.

- Support database server connection to transfer the record of connecting appliance in the network.

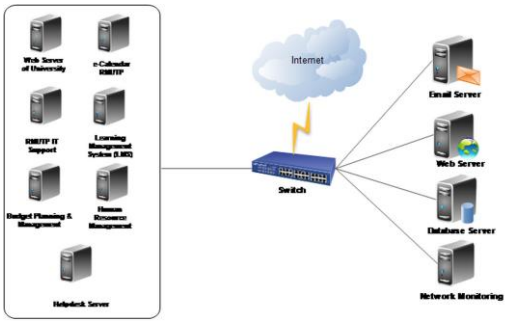

Fig 5. Network Design

- Support the unlimited network appliance monitor.
- Support SMS alert (via Aircard)
- Support e-mail alert
- Support SMS sending record to the system administrator.

2) Database Server stores data such as system administrator information, details of appliance in the network (IP Address, device name, installing location), record of appliance networking check, and record of SMS sending to the system administrator in case of the problem with network connection.

3) Switch connects network with Network Monitoring Appliance and all appliances in the network.

4) Air card links to Network Monitoring Appliance to send SMS to the system administrator.

V. NETWORK MONITORING SYSTEM PROCEDURE

The network monitoring system procedure was demonstrated in Figure 6.

1) Network monitoring system downloads IP Address from Database Server.

2) The system will Ping each IP Address, 30 times in total, in three cases:

- In case of the first network monitoring and the system connects with the terminal appliance by displaying result in a form of Reply from, the network monitoring system is connecting to the appliance successfully. The network monitoring system shall send the connection record to database server.

- If the system cannot connect with the terminal appliance by displaying the result in a form as “Request time out” for 20 times, the Network monitoring system fails to connect with the appliance. Network monitoring system shall connect to Aircard to send SMS and E-mail to the system administrator while sending the connection data and SMS sending record to the database server, and wait for the connection test again. After testing the connection with other network appliances, the system shall re-test the connection again. When the connection is successful, the system will send SMS and E-mail to the system administrator and the database server again to record the SMS sending, the change of appliance connection, and the record of appliance connection to system.

- If the system connects to the unstable terminal appliance and displays result as “Request time out” and “Reply from”, 30 times in total, it means that the connection does not stable all the time. The network monitoring system will connect with Aircard to send SMS and E-mail to the system administrator while sending the connection data and SMS sending record to database server, and wait for the re-test. When the connection is successful, the system will send SMS and E-mail to the system administrator and the database server again to record the SMS sending, the change of appliance connection, and the record of appliance connection to system.

- If the problem arises because of the non-connection to the internal network system and the result displays as “Destination host unreachable”, the system shall send SMS to the system administrator to fix the problem.

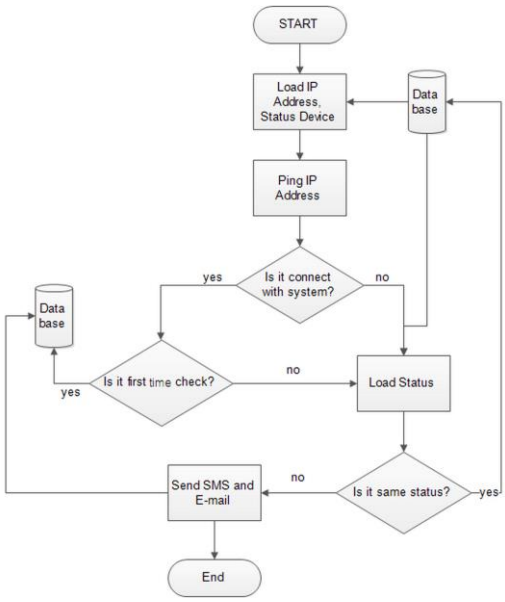

Fig. 6. the network monitoring system procedure

3) The system administrator can monitor the connection of appliance in the network via a website. There are three connection status: Green (online), Red (unable to connect), and Grey (unstable connection).

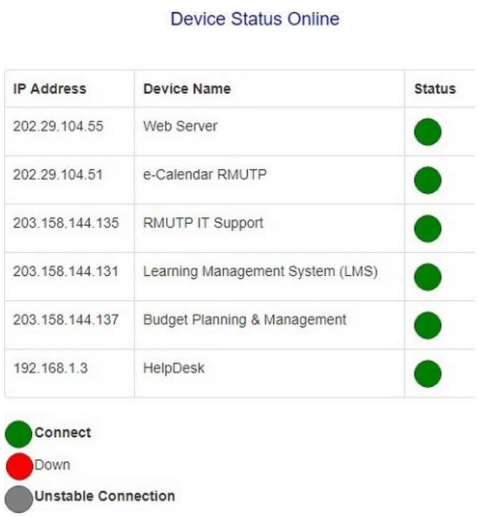

Fig 7. Device Status Online

4) The system administrator can check the record of appliance connection via a website. The designed system will monitor the connection every one hour which allows the system administrator to check the connection record to monitor the possible problem.

5) The system can recheck SMS sending record and send to the system administrator.

VI. RESULTS

The test result of internal system implementation in Rajamangala University of Technology Phra Nakhon shown in Figure 7.

The system operation displays the result on website so that the system administrator can monitor the operation of appliance in the four campuses efficiently. In the alert testing with the simulation of some appliances connecting to the network monitoring system, the system sent the alert E-mail and SMS to the system administrator effectively, as shown in Figure 8,9.

The researcher conducted more test by making the network monitoring system to be unable to connect with the internal system. When testing the connection with the appliance by Ping, the system displayed the result as "Destination host unreachable" and sent SMS to the system administration, as shown in Figure 10.

The comparison of features between the software developing by the researcher and the current software: freeware and software license, as shown in Table I, indicates that the designed and developed software operates efficiently and is sufficient to the demand of university. Table I compares the features of the Software (WhatsUp Gold, The Dude, PRTG, ZENOS) with the developed system's features and functions as follow;

Fig. 8. Sent sms to the system administrator if device cannot connect in the network

A. *Search for Network appliance (Entry 1)*

It is the searching device in the network that connecting with the Network Monitoring Software under the same subnet which is a feature of the developed system in this research. However, the researcher did not activate the feature because the university's IT system service is not only available on the host computer, Access Point and Switch but also a lot of computers for staffs and for classrooms which provides the service from 8 am to 6 pm every day. If the computer is brought into the system after it has been used, the system will always notify. So, the developed system has the same features as the Software WhatsUp Gold, The Dude, PRTG, and ZENOS.

B. *Display the status of an appliance (Entry2)*

It is the connection status of the device in the network monitoring. For the developed system, there was the program development in the form of Web-based so the users can monitor the system through web browse conveniently, as shown in Table 7. The connection status is divided as follow;

Red means no connection with the device or message "Down" is shown after the device's name of the device's IP Address.

Green means connection is succeeded or message "Up" is shown after the device's name of the device's IP Address.

Grey means occasionally connected with the device but not 100% connected.

The connection will be displayed in the form of texts and circle pictures which show the above connection status. The used of Bandwidth also less than Software WhatsUp Gold, The Dude, PRTG, ZENOS that show the connection status in the form of pictures and texts as shown in figure 1 and figure 3.

C. *Display the connection result with the appliance on Web-Base (Entry 3)*

It is the display of the device connected in the network system through Web-Base. The developed system has the Web-Base display so the administrator can monitor the system through Web Browse in the Intranet or Internet network all the time even outside the University which is the same features as in Software WhatsUp Gold, The Dude, PRTG and ZENOS Display connection diagram (Entry 4)

It is the display of the device connected in the network system which monitors with Software (WhatsUp Gold, The Dude, PRTG, ZENOS) in the form of graphics and it is also

compatible with the features display the status of an appliance (Entry 2 of Table 1). Researchers did not develop this feature since the use of internet Bandwidth is quite high when the administrator wants to monitor the connection status of the device through the internet. In the future, the researcher might develop this feature of the system when the user display is adjusted during the use through the internet or intranet.

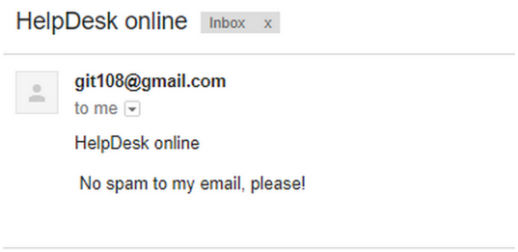

Fig.9. Sent e-mail to the system administrator if device cannot connect in the network

D. Alert the abnormality via E-mail (Entry 5)

It is the notification e-mail when the system is unable to connect with the network device. The developed system will notify in 3 cases as follow;

Case 1: System is unable to connect with the network device.

Case 2: System can connect to the network device but with Unstable Connection which can be seen from the device ping test result as well as display the result as Reply from and Request timeout which reflect the Unstable Connection status of the device.

Case 3: After the case 1 when the system can connect to the device, the system will send email again to notify the successful connection with that device.

For Software WhatsUp Gold, The Dude, PRTG, and ZENOS will notify only two status which is Up and Down. The Up status means the successful connection with the device and Down status means unable to connect with the device. However, the developed system has the notification and also store case 2 data in the database so staffs can analyze the problem as well as a solution for a problem that might occur with the device in the future.

E. Monitor service of Servers (Entry 6)

It is the display of various services that run on the host computer working through SNMP Port which is the feature of Software (WhatsUp Gold, The Dude, PRTG, ZENOS) to check the work of the host computer. For the developed system, this feature was not developed due to pulling the services that run on the host computer need to activate the SNMP Port by set the security system on Firewall of the host computer and it might risk the attack from the Attacker.

F. Search for appliances in multiple subnets (Entry 7)

It is the searching of the device in a network system that belongs to a various subnet which has a connection in the network. The developed system did not activate this feature because the University IT service has many devices which connected through Lan and Wifi and they are not the main devices that need monitoring such as work computer for staff, classroom computer, Tablet, Smart Phone, and Notebook. If the feature is activated, it will cause the system to crash because those devices only work temporarily. These features in the developed system are the same feature in Software WhatsUp Gold, The Dude, PRTG, and ZENOS

G. Alert the abnormality via SMS (Entry 8)

It is the notification SMS sending to staff mobile phone. The developed system brought the SMS feature as the key notification because notification email has limitation concerning the internet network which if the source network (developed system) and/or destination are not available (the staffs' mobile phone), the main center staffs will not receive the notification. In consequence, researcher has recognized the importance of internet limitation in developing such features to solve future problems. Comparing to the features of Software WhatsUp Gold, The Dude, PRTG, and ZENOS that can notify via SMS only when co-operating with devices using SMS Gateway or SMS Gateway system through other providers' API. The API needs to consider the compatibility between the device and software or between software and SMS Gateway system. The system also needs more setting because the software update or the device Firmware that responsible for sending the SMS might stop the software from sending SMS.

The developed system in this research has strong point comparing to other software as follow;

- Notification SMS can solve the problem of internet limitation. If the source network is available and/or users' email at the destination are not available, the main center staffs will not receive the notification email. As such, the developed system also add the notification SMS as one more notification in order to solve such a problem.

Fig. 10. Network Monitoring cannot connect in the network

- It can support an unlimited number of system connection inspecting devices, due to some other software may require payment depend on the number of the device that needs to be monitored. The developed system works with the database to store the data of the

device that need to be monitored. The system will upload the device list to the database before the connection test between the device and system. Whenever a new device is added to the database, it does not need to restart the system to support a newly added device.

- It can record the connection history of the device in the system for problem analysis in the future.
- It can identify the position and location of the malfunctioning device by recording the location data in the database so staffs can acknowledge the location of the malfunctioning device.

TABLE I. THE COMPARISON BETWEEN THE DEVELOPED SYSTEM AND PRESENT SOFTWARE

(✓ means an ability of the software and X means an ability that software cannot operate)

Entry	Performances	WhatsUp Gold	The Dude	PRTG	ZENOS	Proposing research
1	Search for network appliances	✓	✓	✓	✓	✓
2	Display the status of appliance	✓	✓	✓	✓	✓
3	Display the connection result with the appliance on Web-Base	✓	✓	✓	✓	✓
4	Display connection diagram	✓	✓	✓	✓	X
5	Alert the abnormality via E-mail	✓	✓	✓	✓	✓
6	Monitor service of Servers	✓	✓	✓	✓	X
7	Search for appliances in multiple subnets	✓	✓	✓	✓	✓
8	Alert the abnormality via SMS	Function with other appliances and SMS Gateway	Function with other appliances and SMS Gateway	Function with other appliances and SMS Gateway	Function with other appliances and SMS Gateway	✓

VII. CONCLUSION

The designed and developed system operated efficiently at Rajamangala University of Technology Phra Nakhon. The researcher designed and developed the system to support the connection to the external divisions to exchange data and information, and facilitate the system administrator to fix problem promptly. Furthermore, the system administrator was able to monitor the record of network connection via the website and the connection records allowed the system administrator to plan and maintain the appliance to avoid problem. The comparison of developed network monitoring to other software: freeware and software license illustrated that the developed system contained sufficient and efficient features for the university to implement.

ACKNOWLEDGMENT

The research was supported by the annual government statement of expenditure of Thailand (2017) (Thailand Budget Fund)

REFERENCES

[1] Professor Dr. Prapat Thepchatree.(2016).Education Thailand in ASEAN. Retrieved October 8, 2017,http:// www.drprapat.com

[2] Rajamangala University of Technology Phra Nakhon. (2015).Asean community.Retrieved October 8, 2017, http://www.rmutp.ac.th/web 2553/?s=asean

[3] Kim S. Nash and Alyson Behr. (2007). Network Monitoring Definition and Solutions. Retrieved October 8, 2017, https://www.cio.com/article/2438133/networking /network-monitoring-definition-and-solutions.html

[4] Part of the AdEPT Group. (2015). WHAT IS NETWORK MONITORING?. Retrieved October 8, 2017, https:// www.ouritdept.co.uk/what-is-network-monitoring/

[5] Ipswitch Inc. (2016). Retrieved October 8, 2016, https:// www.ipswitch.com/support/documentation#whatsupgold

[6] Network Monitoring. Retrieved October 8, 2016, https:// www.whatsupgold.com/

[7] Ipswitch, Inc. WhatsUP Gold User's Guide Software Version 8. United State

[8] PAESSLER AG. (2010). Managing Central Monitoring in Distributed Systems White Paper. Germany

[9] PAESSLER AG. (2010). PRTG NETWORK MONITOR. Retrieved October 8, 2017, https://www.paessler.com/prtg

[10] Latvian company.(1996).The Dude.Retrieved October 8, 2017, https://www.mikrotik.com/thedude

[11] Latvian company. The Dude 4 Documenttation. Jul 14, 2010. Lavita

[12] Zenoss Inc. NETWORK MONITORING. Retrieved October 8, 2017, https://www.zenoss.com/product/ unified-monitoring/network-monitoring

[13] Zenoss Inc. (2009). Zenoss Enterprise Architecture Overview. United State

[14] Internet Control Message Protocol (ICMP) | Computer Networks. Retrieved October 8,

2017 ,https://www.geeksforgeeks.org/internet-control-message-protocol-icmp/

[15] Professor Godred Fairurst. (2010).Internet Control Message Protocol (ICMP) .Retrieved October 8, 2017, https://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/icmp.html

[16] INTRODUCTION TO THE ICMP PROTOCOL. Retrieved October 8, 2017, http://www.firewall.cx /networking-topics/protocols/icmp-protocol/151-icmp-introduction.html

[17] IMPERVA. PING FLOOD(ICMP FLOOD). Retrieved October 8, 2017, https://www.incapsula.com/ddos /attack-glossary/ping-icmp-flood.html

[18] CLOUDFLARE. Ping (ICMP) Flood DdoS Attack. Retrieved October 8, 2017, https://www.cloudflare.com /learning/ddos/ping-icmp-flood-ddos-attack/

[19] F5. ICMP Flood, Ping Flood, Smurf Attack. Retrieved October 8, 2017, https://f5.com/glossary/icmp-flood-ping-flood-smurf-attack