Network management system based on the functional model of the IETF: SNMP, to monitor the resources of the network EMAPA-I's LAN

Edgar A. Maya, Richard A. Mallamas

***Abstract.*- The present project consists to designing a monitoring system based on the functional model "SNMP"by using Open Source tools in a network server provided by EMAPA-I with the intention of obtaining a knowledge base on the incidents that arise, facilitating the network administrator to take remedial measures in time the devices are more susceptible to failures.**

Indexed terms.- SNMP, CentOS, GLPI, OCS-INVENTORY, IP.

I. INTRODUCTION

EMAPA-I is an enterprise that strives daily to maintain high levels of management in the provision of efficient basic services, quality and continuity, obtaining every year to increase the number of its customers, so that it is currently strengthening its technological infrastructure gradually with the purpose of improving the provision of services for the benefit of the community. Currently the systems department is located in the start-up phase to the search of a software that enables you to monitor the computer resources that are within their LAN network, therefore have not yet been established policies and processes to ensure both the reliability of the information as the availability in the communications network, causing economic losses to the institution by the interruption in the network.

This research document received in December 2015 was conducted as a preliminary project for the professional degree in Engineering in Electronics and Communication Networks Engineering Faculty of Applied Science (FICA) at the Técnica del Norte University

E.A. Maya, professor at the Tecnica del Norte University, in the Engineering in Electronics and Communication Networks, Av. 17 de Julio sector El Olivo, Ibarra-Ecuador (phone 09-85198-101; e-mail: eamaya@utn.edu.ec)).

R.A. Mallamas, graduate of the School of Engineering in Electronics and Communication Networks (phone 09-85155-075; e-mail: richard_mallamas@hotmail.com).

The progressive increase of users hinder to resolve the problems encountered by network congestion, same that is caused by exceeding performance thresholds solution. Also they do not have tools to perform tasks handling, control and registration of notifications that alert on the status of communication devices, for this reason failures not be detectable in time, causing the discomfort of staff working within the institution.

This whole series of problems have gradually affecting the efficiency of the data network, because the organization lacks procedures to allow deployment failures in real time or perform continuous monitoring using statistics to assess the performance of communications resources. The technological growth EMAPA-I must guarantee the reliability of the data network, so the implementation of a model-based management system will establish maintenance policies designed to ensure the availability of the LAN of the institution

II. DEFINITIONS AND BASIC CONCEPTS

A. Network Management.

Network management includes the deployment, integration and coordination of the hardware, software and human elements to monitor, test, polling, configure, analyze, evaluate and control the resources of the network to achieve the requirements of real time, operational performance and quality of service at a reasonable price.

B. Elements of network management

In the network management there are two types of entities: manager and agent, between which information is exchanged for a diagnosis of network.

Molero, L. (2010) mention that a manager is a server that is running some type of software system that can handle the administration tasks for a network, is responsible for the choice and receive scans of the traffic of agents. The manager is that performs an inquiry in particular to know the specific status of one or multiple computers within the network in order to detect irregularities

The second entity, the agent is a software within the device that you want to manage. Due to the great com-

plexity presented the networks currently, manufacturers add agents in their computers to allow flexibility in the management of network. The agents are those who perceive any inconsistency within the device, and sends a message to the manager to alert you to their current situation.

Today, the majority of the IP devices come with some type of embedded SNMP agent, the fact of the suppliers of devices are ready to deploy agents in many of its products greatly helps the system administration.

C. Management model SNMP

IETF is a working group with an informal organization that contributes to the engineering and evolution of Internet technologies, which has the responsibility of developing Internet standards; has defined a network management model consists of four functional areas, which are shown in figure 1.

Figure 1.- Management model SNMP

Below describes the basic functions that satisfies each one of these areas:

Operation function.-It comprises the execution daily and continues the network includes activities such as auditing, discovery and monitoring of the network to ensure that everything is running correctly. (Alexander Clemm, 2007).

Management function.- Includes the support functions required to manage the network, includes activities such as the design of the network, tracking its use, address assignment, planning upgrades to the network, receiving service orders associated with end users and customers, inventory tracking of network. (Alexander Clemm, 2007).

Maintenance function.- Includes the functionality to ensure the operation of the network and communication services as expected. This includes activities such as diagnostic, troubleshooting, and repair of components that do not work according to what was planned, in order to maintain the network in a state in which it can be used continuously and providing the appropriate service. (Cátedra redes de información, 2010).

Security function.- Includes features such as to maintain and manage the access control information, detection of security incidents, to identify the main risks and threats that affect the most critical servers. (Cátedra redes de información, 2010).

D. Simple Network Management Protocol (SNMP)

SNMP is based on the paradigm manager-agent, is an application layer protocol based on the TCP/IP architecture, which makes possible the exchange of management information between network devices, its operation is described in figure 2, where it can be appreciated as interact their main components that are: agent, simple network management protocol (SNMP) and the management information base (MIB).

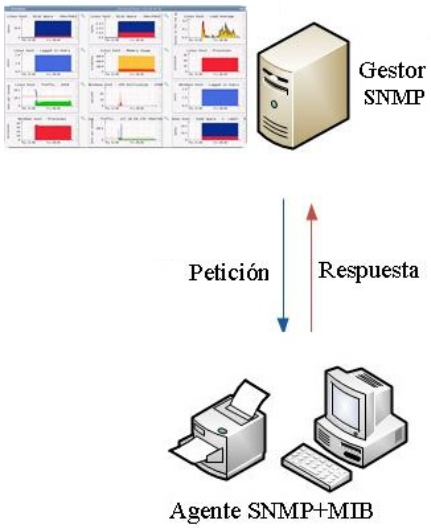

Figure 2.- Elements of network management SNMP

At present there are three versions of the SNMP protocol defined as: SNMPv1, SNMPv2 and SNMPv3.

SNMPv1 constitutes the first definition and implementation of the SNMP protocol, being described in RFC's 1155, 1157 and 1212 of the Internet Engineering Task Force (IETF), in which account with basic functions both configuration and security. SNMPv2 offers several monitoring operations, with simple setup, which are compatible with the majority of current network devices. However in the version 3, adds better security, authentication, and access control.

III. CURRENT SITUATION OF THE NETWORK EMAPA'S LAN

The infrastructure available in EMAPA is centralised in the virtualization of services, is currently composed of the following technological infrastructure:

A. Telecommunications room

The telecommunications room is located on the first floor of the building, here are the routing and switching equipment as well as the servers, which are mounted in standard racks of nineteen inches. The equipment room is administered by the Department of Information Technologies and Communication, which is responsible for carrying out the maintenance and verification of the correct functioning of the technological infrastructure.

B. Servers

The servers are of vital importance for the proper functioning of the institution of the bank of servers, some have are external support, while the following are in charge of the Department of Informatics:

Table I.
Servers that have the maintenance department of informatics

Trademark	Server	Importance
HP PROLIANT		High
Virtualized server	Active Directory-Antivirus-DNS	High
Virtualized server	Correo	High
RouterBoad Mikrotik 1100AHx2	Router-Firewall-DHCP	High

The analysis for the choice of the virtual servers was conducted taking into account the availability of functioning of the services provided by each of them within the Entity.

C. Network topology

The network is located in star topology, where account with switches as central distributors and a firewall. The building of Emapa-I has 4 floors which counted with UTP cabling for the connection between the departments with which account every floor. The horizontal cabling of the institution is of type UTP category 6 and 5e, which are installed in the fourth of computers, servers, and in the departments of the institution respectively.

D. Network diagram

The network scheme with which account the company incorporates a device firewall, in addition to a Cisco switch that binds the virtual networks with the firewall as well as shown in the following figure:

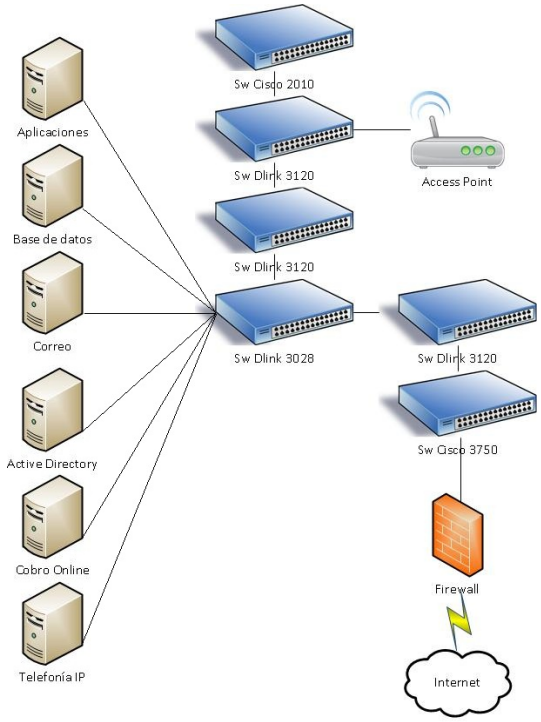

Figure 3.- Network diagram EMAPA

IV. MANAGEMENT OF THE NETWORK EMAPA'S LAN

A. Establishment of policies for management of computing resources in Emapa-I

Below is the network management policies evaluated from the SNMP management system, a systematic audit to the Department of computing resources and the internal control standards for information technologies which are designed to expand the level of security and better fulfill the objectives of the Department of informatics.

Organizational Levels

a) Boss of Technological Infrastructure.- Ensure the maintenance of a high availability and correct functioning of computing platforms that support the activities of Emapa-I for users.

b) Computer Analyst 1.- Implement and coordinate activities of technical support and maintenance of computer equipment, information and communication technologies

c) Computer Analyst 2.- Implement and coordinate activities of technical support and maintenance of computer equipment, information and communication technologies

Validity

The document described with the policies on the management of the network will be in effect at the time that it would be adopted as a technical paper by the relevant authorities of Emapa-I. This rules should be revised and updated according to the changes in the infrastructure

that can be presented to the institution.

In the absence of a specific standard for network administration, the management policies are made on the basis of the SNMP management model, established by the IETF:

1. Policy for the management of the data network
   1.1. Objective of the Management Policy
   1.2. Commitment of the Authorities.
2. Operation Management.
   2.1. Network Inventory
   2.2. Equipment configuration.
3. Administration Management.
   3.1. Maintenance of the inventory and income.
   3.2. Help Desk.
4. Maintenance Management
   4.1. Monitoring Parameters
   4.2. Handling Bugs.
   4.3. Reports
5. Security Management.
   5.1. Access Management Software.
   5.2. Access to network devices.

B. Implementation of management tools in the network EMAPA's LAN

This area of management comprises in the analysis of the current situation of the data network of Emapa-I for the logical and physical state in which it is located.

Requirements for election management software

Within this area of management is necessary to perform a preliminary comparative analysis of the functionality and better software features of management, has been selected Zennos, Zabbix, Cacti And Nagios. The management software was elected on the basis of the IEEE standard 29148, taking as a reference the compliance of the SNMP management model and the needs of the Entity

The tool was chosen Zabbix by the characteristics that were evaluated, one of the main needs which justified its use was that the computing department request a platform that is configurable in its entirety by means of a graphical interface. In addition the equipment to monitor can be found in its entirety with Windows operating system, and Zabbix gives many options to get data from this S.O., also provides establishment of thresholds that generate alerts when they arrive at their maximum operating limit and send email notifications.

Operation function of the SNMP Model

The entity did not have a record of inventory of computers and network configurations so that if there was failure in some device is lost information, and reconfigure without a backup decreased network availability.

Therefore in the function of operation was the discovery and inventory of computers, we help the tool: Open Computer and Software Inventory Next Generation (OCS-NG) which is a free software that allows users to manage support the inventory of the assets of the network based on a client-server model among which are exchanged information to obtain a diagnosis, compiling the information for the software and hardware installed on the computers in our network in a centralized system.

Management function of the SNMP Model

The technical staff complies with activities within and outside the institution, so that if a team of network failed and the technicians were not, the network availability depended for technicians to return to give a solution to that incident and similarly problems of staff members were not treated promptly.

It is for this reason that the administration functions that are covered are focused on the implementation of a system of incidents. It chose the GLPI tool which works in the following way: the functionary enters the web platform and emits the incidence that can be related to: problems entering the internet or integrated printing problems, damage to the mouse, keyboard, phone, monitor, and damages related to computing resources in general, for its part the support team, will receive the incidence both by the web platform as by mail, and according to the urgency of the problem is take appropriate considerations to resolve the incident, which is stored in a database for both get reports on the actions taken to make a follow-up to the incidence produced.

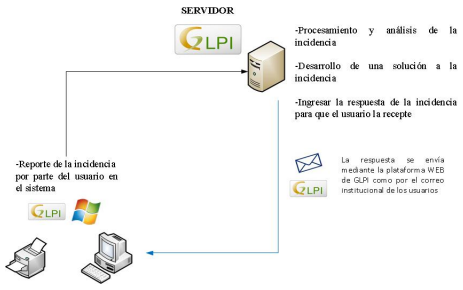

Figure 4.- GLPI operation in Emapa-I

Maintenance function of the SNMP Model

By not having a control of the capabilities of both the hard disk, bandwidth, ram, or interfaces of the servers, if these features are overloading, caused delay in the availability and reliability of the data network until turning functional again, and if played to replace any component is produced an expense not planned

In such a way that made the monitoring of the teams of routing and servers described above in order to determine the behavior of the network, then presents the structure of correction of failures that we continue in the institution.

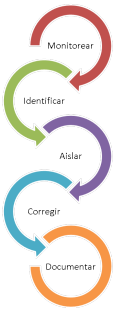

Figure 5.- Process of failure detection in EMAPA-I

Monitoring of alarms.- By monitoring the network with the Zabbix Platform, we can identify what equipment you have some problems and then set alarms that tell us feature of the team is the one that requires more attention, it should be considered to set alarms to only tell us a state critical, it is not very convenient, since the response time to give a solution is not always immediate, for this reason you will need to provide a level of alarms that notify the administrator long before an incident occurs, or assess minor faults constants to prevent more serious problems in the future. (Alexander Clemm, 2007).

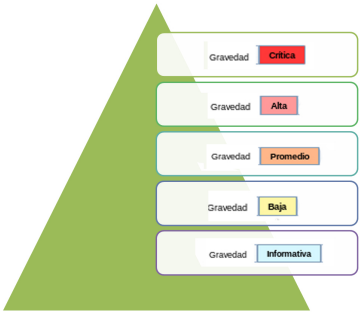

Figure 6.- Levels of severity in the platform Zabbix

Identification of the failure.- At the time that is an incident in the network computers, you will proceed to find the cause of the source of the problem, the initiators of alamas that show us the platform Zabbix, will help us to find the computer that generated the incidence, but to solve needs additional tests which will depend on knowledge of network administrator so that he can propose possible solutions, the monitored equipments presented the following characteristics.

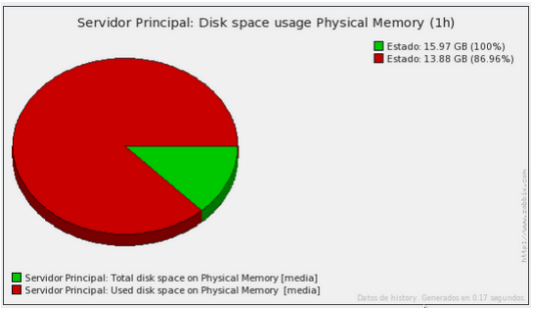

Figure 7.- RAM space in the Active Directory Server

We can point to several teams with critical severity level, which were reviewed and verified that they had a high consumption in both the RAM.ªnd "hard disk", capabilities that generate a notification email to your network administrator.

Likewise, the analysis bandwidth traffic LAN is done, where I found that there are indexes use bandwidth rise rather than fall, and this happens because most users use the data network to upload files to the different systems of the EMAPA-I.

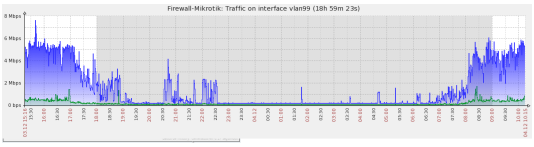

Figure 8.- Network traffic on the data VLAN

Insulation.- It should be borne in mind that the teams who have any inconvenience critical affect drastically to the operation of network, this is why we should have a document based on the configuration of the computers or buy a device that can support to help solve the problem by a certain time, in such a way as to decrease the impact of failure on the data network. (Dolores Gómez, 2014).

Correction of the Failure.- To give a correction to the failure must be take into account the gravity of the same and the availability of resources that is placed in the company, among the most common actions you can submit the following:

- Replacement of resources, either only the affected part or in its entirety.
- Install updates related to the incident submitted
- Restart or settings for one or more specific parameters in the network equipment

Documentation.- The data that is generated by Zabbix are continuously stored in a database, and this information may help the network administrator to document it either in the incidences of GLPI system, or any other platform that decides, since this activity will depend mainly on the IT department.

Security function of the SNMP Model

In the security feature will be oriented to reduce the possibility of incidents, therefore, in the tools that were installed took into account the following observations, while for the other teams that are located in the data network is left as a recommendation to continue.

- Assignment of privileges to access only those persons who need a steady income either to obtain reports or enter new equipment to the monitoring system.
- Enter a strong password that integrates letters, numbers and symbols, so they are harder to breach.

- Perform a password change of robust way to computers that are in charge of every 6 months
- Have a restore point of the teams in the event of any failure to have a backup of the data obtained

A. Monitoring by the snmpv3 Protocol

In the SNMP version 3 are used fields that allow both authentication and encryption of passwords, to perform the monitoring. Unlike previous versions of SNMP is no longer uses the concept of community, which was changed by the field of users. In addition account with the encryption feature of the packet that is sent to be processed with the manager, making it more difficult for an attacker wants to infiltrate data with a software to deploy the network traffic, as it was found in tests.

B. Restriction of web pages

Once you have documented the data network, it is necessary to deny certain web pages according to the policies described; which were established through the study of the current situation; in view that decrease the performance of the network and it is very common to perform installation of involuntary virus through these platforms.

The configuration of these rules allowed to control the data traffic that runs daily through the network. In this way also indicated the advantages of taking advantage of all the functions with which have the computers that are located within the Institution.

V. MANUAL OF PROCEDURES

Introduction

The Department of computing resources aims to contribute to the maintenance and improvement of the technological infrastructure, which are the fundamental support for the good management, operation, structure and organization of the institution. At present there is a great variety of methods in which build to present a manual of procedures, but due to the importance that have both public and private entities must be comply with standards that guarantee uniformity in both the content, as its form of presentation, it is for this reason that the present manual is based on the ISO.

Procedures Manual-Operation function

- Objective.- Provide the information to monitor the configuration of network equipment and servers to be monitored
- Scope.- Will indicate the processes that allow the configuration of the network equipment and servers to add to the management system, will be presented the processes that allow us to add the end user computers to inventory system.

Procedures Manual-Management function

- Objective.- Provide information about the follow-up to the initial inventory and reporting of incidents on the part of the final user through helpdesk
- Scope.- This function relates together both with the management of operation as the management of maintenance, therefore here determines the monitoring of components of the devices already inventoried and it will also explain the way in which we will receive the incidents that report the end users.

Procedures Manual-Maintenance function

- Objective.- Establish processes that allow for the revision of the thresholds that generate specific notifications, which are a basis for analysing and identifying the failures that occur in the monitored equipments.
- Scope.- Set the thresholds that computers to manage must maintain, and if they are exceeded, the technicians responsible should seek a solution in a timely manner allowing offer a high level of continuity in the network.

Procedures Manual-Security function

- Objective.- Provide security to the system of management by the authentication and income not transferable to the users in the department of computing resources to ensure the integrity of the information
- Scope.- Supervise and monitor the changes in the system of management by reviewing the threats or modifications not documented, preventing unauthorized access to information.

VI. CONCLUSIONS

To analyze the institutional requirements using the functional areas of the SNMP model could be found shortcomings as: not having an updated inventory, not having control of the technical capabilities of its devices, nor documentation of policies to ensure the reliability of the information of your computing resources; it can be noted that this model gives a series of steps well organized to that technical staff can accurately identify the aspects that decrease the performance of the network in order to be solved in time

The monitoring of the computers on the network of Emapa-I is conducted through the snmpv2 protocol, since that was easy to deploy both for the network equipment such as servers of the entity; it was also set up an alarm system to indicate to the technical department that the thresholds established in the capacities of both bandwidth consumption, RAM and hard disk are surpassing, substantially diminishing the response time in giving a solution.

The tools that are involved in this project are oriented to free environments, took into account the institutional requirements analyzed based on the specification of the standard IEEE 29148, which allowed to have a broad perspective on aspects such as the detection of errors, documentation and maintenance of installed platforms, fundamental characteristics to meet the stated objectives.

Tests were carried out for operation of installed platforms which helped to develop and maintain an updated inventory, bring the control of the technical capabilities of the devices and set security policies, which are the basis for fulfilling the institutional objectives that include activities such as: Preparation of technical reports, perform schedules and organize its technological infrastructure, taking into account standards that help to ensure the availability of resources within the Institution

Configured a tool that permits a control of incidents, since it is not maintained a coordination and documentation of the solutions that the functionary requested the Department of Informatics, allowing deliver more detailed reports of the activities carried out by this department, in addition to improving the support processes to users giving a margin of approximately 10 minutes in giving a solution to the incident.

Simulation tests were conducted of overload of thresholds established in the capacities of both bandwidth consumption, RAM and hard disk was also revised the format of sending and receiving of incidents to check that both the alarm system to email as the settings are in correct operation.

Information was gathered about the security features of snmpv3 protocol which was verified by an analysis of protocols with the platform Wireshark, in where they demonstrated the encryption and authentication of monitored packages to the institution, indicating the benefits that the internal and external attacks can be avoided in a timely manner.

To strengthen the study of the protocol snmpv3 is executed operation tests in the financial department of the institution, where they established thresholds that indicate when the capacities of both hard disk, or RAM are overloaded; in addition to verify the encryption is used the Wireshark tool with which demonstrated that the encryption and authentication settings in the devices are operating correctly.

Through the implementation of the platforms for the inventory system, the system of incidents, and the monitoring system is managed to develop the manuals of procedure on the basis of the areas of the model of SNMP Management, which are a set of instructions that guides the technical staff to maintain the data network of the updated entity and in constant monitoring, thus ensuring the availability of operating their computing resources.

According to the results obtained in the current situation where highlights shortcomings as: Not having an updated inventory and not have control of the technical capabilities of its devices; policies were established to cover the functions of the SNMP management model which has certain guidelines that allow the network administrator to manage the computing resources of the institution of an efficient, generating significant changes, since by means of these policies and procedures will be displayed as an entity that offer services with continuity and quality to the community.

REFERENCES

Subramanian, A & Timothy A. (2010). Network Management. 2da edición. Sitio de Publicación: Pearson Education India

Douglas, M. & Schmidt K. (2009). Essential SNMP. 2da. Edición. Sitio de publicación: O'Reilly Media.

Molero, L. & Villaruel M. (2010). Planificación y gestión de red. Recuperado el 14 de febrero del 2015 de: http://www.urbe.edu/info-consultas/web-profesor/12697883/archivos/planificacion-gestion-red/Unidad-I.pdf

Orozco P. (2010). Gestión y organización de sistemas y redes de comunicaciones en el departamento de T.I. Recuperado el 15 de febrero del 2015 de: http://www.slideshare.net/pakus/gestion-de-red

RFC 1901. (1996). Introduction to Community-based SNMPv2. Recuperado el 10 de marzo del 2015 de: https://www.ietf.org/rfc/rfc1901.txt

RFC 2578. (1999). Structure of Management Information Version 2 (SMIv2). Recuperado el 10 de marzo del 2015 de: https://www.ietf.org/rfc/rfc2578.txt

RFC 2570. (1999). Introduction to Version 3 of the Internet-standard Network Management Framework. Recuperado el 5 de abril del 2015 de: https://www.ietf.org/rfc/rfc2570.txt

RFC 3411. (2002). An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks. Recuperado el 10 de abril del 2015 de: https://www.ietf.org/rfc/rfc3411.txt

Born in Ibarra province of Imbabura on April 22, 1980. Computer Systems Engineer of the "Universidad Técnica del Norte" in 2006. Today, teaches in the Electronics and Communication Network Engineer Career at the UTN, Ibarra – Ecuador, obtained the Master in Communication and Networks, Pontificia Universidad Católica del Ecuador, Quito – Ecuador.

Born in Atuntaqui on September 21, 1987. He studied in the "Mariano Suarez Veintimilla"High school, in 2006 obtained his Bachelor of Commerce and Administration specialty computer applications. Then he studied Electronics and Communication Network Engineer at the "Universidad Técnica del Norte", Ibarra-Ecuador.